# DA – Espionage – HSS

### Notes

The cards under “2NC – Impact – Asia Prolif” and “2NC – Impact – Economy” were taken from the elections file

I found a counterplan that purports to solve the aff with the espionage DA as a NB – the counterplan reforms what “covered transaction” means in the context of CFIUS, which changes CFIUS’ authority – I didn’t cut any aff answers because Repko told me to focus on the DA, but I think that the counterplan is slightly more beneficial because not only does it resolve the link, it resolves some of the uniqueness issues with the disad as well

The aff arguments that 1) the US military is miles ahead of the Chinese army and 2) there’s massive espionage going on now, which should non unique the disad, are going to be hard to beat. I think the best neg responses, then, are:

Superiority’s not inevitable if we win China can steal and develop the latest U.S. military tech, because then Chinese forces can become technologically equal to the U.S. – that also answers their espionage now arguments, because regardless if they’ve stolen tech before, a key variable to determine U.S. military superiority is recent innovations in military tech, which means that only future theft can allow Chinese military growth and innovation

#### Some good history about CFIUS’ authority and the Ralls case

Stanley 15 – (Mary Ellen Stanley, B.A., University of Richmond (2011); M.A., Baylor University (2013); J.D., Brooklyn Law School (Expected 2016); Editor-in-Chief, Brooklyn Journal of International Law (2015-2016); Fellow, Dennis J. Block Center for the Study of International Business Law (2014-2016); 2015, “From China with Love: Espionage in the Age of Foreign Investment,” Published in *Brooklyn Journal of International Law*, Vol.40, Issue 3, pgs 1033-1079; <http://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1113&context=bjil>, Accessed 6/24/16, HWilson)

In March, 2012, Ralls Corporation (“Ralls”), a Delaware corporation owned by Chinese executives, acquired four Oregon-based limited liability companies that were formed to develop wind farms. 2 The wind farms were located “in and around” a restricted U.S. Navy (“Navy”) airspace and bombing site. 3 Once the acquisition was complete, the Navy notified Ralls that it was concerned about the location of one of the wind farms.4 Although Ralls moved the contested wind farm, the Committee on Foreign Investment in the United States (“CFIUS” or the “Committee”) compelled Ralls to file a notice with CFIUS to review the transaction.5 After CFIUS investigated the transaction and attempted to mitigate the national security concerns,6 CFIUS submitted its report and recommendation to President Obama.7 On September 28, 2013, President Obama mandated Ralls divest all property interests in the project companies, terminate access to the project site, and refrain from selling the project companies to third parties.8 Neither CFIUS nor President Obama notified Ralls of the evidence supporting their decisions, and Ralls was never given an opportunity to rebut the evidence.9

After President Obama mandated that Ralls unwind the acquisition (the “Presidential Order”), Ralls became the first party to challenge CFIUS’s authority and the Presidential Order in court.10 On July 15, 2014, the United States Court of Appeals for the District of Columbia issued a controversial decision in Ralls Corporation v. Committee on Foreign Investment in the United States and held that the Presidential Order deprived Ralls of its property interests in the companies without due process.11 Subsequently, in an unprecedented decision, 12 the D.C. District Court ordered CFIUS to provide Ralls with the information that supported the Presidential Order to unwind Ralls’ acquisition of the wind farm companies.13 The Ralls decision illustrates an ongoing conflict between foreign investors and the CFIUS review process. Additionally, the decision revived the debate about the efficacy and integrity of the mysterious reviews that consistently plague foreign direct investment (“FDI”) into the United States.14

## Negative

### 1NC – DA

#### Chinese espionage is coming now – they’re targeting microchip technology and semiconductors

Mozur and Perlez 16 – (Paul Mozur writes about technology from The Wall Street Journal's Beijing bureau. His coverage areas include companies such as Foxconn, Huawei and Tencent and industry topics such as social media, censorship and China's electronics supply chain; Jane Perlez is the chief diplomatic correspondent in the Beijing bureau of The New York Times. She covers China and its foreign policy, particularly relations between the United States and China, and their impact on the Asian region; 2/4/16, “Concern Grows in U.S. Over Chinas Drive to Make Chips,” <http://www.nytimes.com/2016/02/05/technology/concern-grows-in-us-over-chinas-drive-to-make-chips.html?_r=1>, Accessed 6/27/16, HWilson) \*\*\* cites Mark Newman, a Sanford C. Bernstein analyst, and Colin Humphreys, a British physicist at Cambridge University

Advancing its chip industry has been a major political initiative for Beijing. In recent years, analysts said, Chinese corporate espionage and hacking efforts have been aimed at stealing chip technology, while Chinese firms have used government funds to buy foreign companies and technology and attract engineers.

Last year, different subsidiaries of the state-controlled Tsinghua Holdings made a number of bids for American companies, including an unsuccessful S23 billion offer for the American memory chip maker Micron Technology and a $3.78 billion bid for a 15 percent stake in the hard-drive maker Western Digital, which was accepted.

Last year's spree of deal activity, and lack of American regulatory response, spurred a Sanford C. Bernstein analyst, Mark Newman, to say in a November report that the United States "runs the risk of being asleep at the wheel." He cited efforts by South Korea and Taiwan to prevent China from acquiring some technology assets.

The Lumileds block is being interpreted by the chip industry as the United States "waking up a bit to the threat," Mr. Newman said in an email. Gallium nitride is particularly sensitive. One military industry magazine called the material tire biggest tiring since silicon, which is now commonly used to make tire transistors in microchips. It cited Raytheon's use of tire material to make smaller, low-powered radar for American missile systems. "Many say it's tire most important semiconductor material since silicon," said Colin Humphreys, a British physicist at Cambridge University.

He said that while it was not clear what tire United States government was worried about, research by LED companies into technology linking gallium nitride and silicon could have broader implications for creating advanced microchips that could be used in a wide array of electronics.

Tire would-be investor in Lumileds, GSR Ventures, also holds a stake in Lattice Power, a Chinese company that has been vocal about its efforts to develop technology related to gallium nitride and silicon.

In a November 2015 statement about a recent investigation into Chinese industrial espionage, Taiwan's Ministry of Justice also expressed worries about China aiming at tire material. Calling tire mass production of gallium nitride a "key development project" for China, tire ministry said it was concerned about tire theft of trade secrets from Taiwanese companies working on tire material and Chinese-led recruitment of engineers knowledgeable about it.

#### Increasing CFIUS transparency makes effective counter-espionage in the future impossible

Stanley 15 – (Mary Ellen Stanley, B.A., University of Richmond (2011); M.A., Baylor University (2013); J.D., Brooklyn Law School (Expected 2016); Editor-in-Chief, Brooklyn Journal of International Law (2015-2016); Fellow, Dennis J. Block Center for the Study of International Business Law (2014-2016); 2015, “From China with Love: Espionage in the Age of Foreign Investment,” Published in *Brooklyn Journal of International Law*, Vol.40, Issue 3, pgs 1033-1079; <http://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1113&context=bjil>, Accessed 6/24/16, HWilson)

A. Maintaining a Permissive Definition of “National Security”

Contrary to the suggestions of recent scholarship and proposed legislation, the term “national security” must not be explicitly defined. Even though commentators suggest a need for a definition that expands CFIUS’s scope of power or increases the Committee’s transparency to foreign investors,240 providing a concrete definition inhibits CFIUS’s ability to adapt to new forms of industrial espionage. Such fixed definitions would likely overlook nuanced threats in the current era of globalization and compromise the nation’s security. In order to properly maintain national security within the United States, the definition of “national security” should not be concretely defined. Instead, “national security” should remain a broad term, in order to best grapple with unexpected issues. As seen in § 2170(f), ten of the eleven factors the Committee considers are explicitly focused on inquiries concerning national security.241

Additionally, the definition of “national security” must not be specifically defined to include “economic security” or a “net benefit” review.242 Including “economic security” as part of the national security inquiry would insert a political factor into CFIUS’s jurisdiction and thus politicize the review process. Although CFIUS, in both its structure and history, often appears to conflate national security with economic security, it is important to note that national and economic security are often tightly intertwined. This close relationship is proven by CFIUS’s intimate relationship with the Department of the Treasury and due to CFIUS’s jurisdiction hinging on the type of economic transaction.243 Although the economic security of the nation is critical, economic security should not eclipse the foundational concern of CFIUS—national security.244

If the substance of CFIUS national security inquiries were amended to include a “net benefit” review, as proposed in Congresswoman DeLauro’s legislation, the analysis would become even more politicized because subsequent evaluations would range into more politically-debated national issues. 245 Topics such as “economic activity,” “quality of employment,” the effect on productivity, “industrial efficiency,” and compatibility with “U.S. cultural policies” 246 would lead to drastic politicization of the review process. These issues would also divert CFIUS’s focus from its already burdensome task of protecting national security. Furthermore, a substantive expansion of the national security inquiry would not only discourage FDI, but would make the CFIUS judgments more arbitrary and politicized due to the critical lack of a framework for determining what constitutes a “net benefit.” Finally, as seen in the Chinese Model, which arguably violates China’s WTO commitments, adding such stipulations could possibly violate the United States’ commitments247 to the WTO.248

#### Successful tech espionage leads to Chinese military superiority

Mozur and Perlez 16 – (Paul Mozur writes about technology from The Wall Street Journal's Beijing bureau. His coverage areas include companies such as Foxconn, Huawei and Tencent and industry topics such as social media, censorship and China's electronics supply chain; Jane Perlez is the chief diplomatic correspondent in the Beijing bureau of The New York Times. She covers China and its foreign policy, particularly relations between the United States and China, and their impact on the Asian region; 2/4/16, “Concern Grows in U.S. Over Chinas Drive to Make Chips,” <http://www.nytimes.com/2016/02/05/technology/concern-grows-in-us-over-chinas-drive-to-make-chips.html?_r=1>, Accessed 6/27/16, HWilson) \*\*\* cites Mark Newman, a Sanford C. Bernstein analyst, and Colin Humphreys, a British physicist at Cambridge University

HONG KONG — China is spending billions of dollars on a major push to make its own microchips, an effort that could bolster its military capabilities as well as its homegrown technology industry.

Those ambitions are starting to be noticed in Washington.

Worries over China's chip ambitions were the main reason that United States officials blocked the proposed purchase for as much as S2.9 billion of a controlling stake in a unit of the Dutch electronics company Philips by Chinese investors, according to one expert and a second person involved with the deal discussions.

The rare blockage underscores growing concern in Washington about Chinese efforts to acquire the know-how to make the semiconductors that work as the brains of all lands of sophisticated electronics, including military applications like missile systems.

In the case of the Philips deal, the company said late last month that it would terminate a March 2015 agreement to sell a majority stake in its auto and light-emitting diode components business known as Lumileds to a group that included the Chinese investors GO Scale Capital and GSR Ventures. It cited concerns raised by the Committee on Foreign Investment in the United States, which reviews whether foreign investments in the country present a national security risk.

Philips said that despite efforts to alleviate concerns, the committee — known as Cfius — did not approve the transaction.

"There is a belief in the Cfius community that China has become innately hostile and that these aren't just business deals anymore," said James Lewis, a senior fellow at the Center for Strategic and International Studies, a research firm, who speaks to people connected with the committee's process.

Philips did not respond to requests for comment. GSR Ventures, which sponsors GO Scale Capital, declined to comment.

Cfius, an interagency body that includes representatives from the Treasury and Justice Departments, declined to comment and does not make its findings public.

Cfius reviews have been a growing problem for outbound Chinese deals. According to the most recent data available, in 2012 and 2013 Chinese investment accounted for more committee reviews than money coming from any other country. A 2008 Chinese effort to invest in the network equipment company 3Com was withdrawn while the committee was reviewing it.

Recently, the committee found acceptable a number of major Chinese deals, including a takeover of Smithfield Foods by Shuanghui International and Lenovo's takeover of IBM's low-end server unit. In 2012, President Obama ordered a Chinese company to stop building wind farms near an American military installation in Oregon after a negative Cfius review.

At the center of the committee's concerns on the Philips deal, according to Mr. Lewis, was a little known but increasingly important advanced semiconductor material called gallium nitride. Though not a household name like silicon, gallium nitride, often referred to by its abbreviation GaN, could be used to construct a new generation of powerful and versatile microchips.

It has been used for decades in the low-energy light sources known as light- emitting diodes, and it features in technology as mundane as Blu-ray Disc players. But its resistance to heat and radiation give it a number of military and space applications. Gallium nitride chips are being used in radar for antiballistic missiles and in an Air Force radar system, called Space Fence, that is used to track space debris.

"Gallium nitride makes better-performing semiconductors that were key in upgrading Patriot radar systems," said Mr. Lewis. "It's classic dual use, sensitive in that it could be used in other advanced weapons sensors and jamming systems."

#### Chinese military superiority causes Asian instability and regional proliferation – incites territorial grabs which escalate to US-China nuclear war

Colby 14 – (Elbridge Colby is the Robert M. Gates Fellow at the Center for a New American Security, 12/19/14, “Welcome to China and America's Nuclear Nightmare,” *National Interest*, <http://nationalinterest.org/feature/welcome-china-americas-nuclear-nightmare-11891?page=show>, Accessed 6/27/16, HWilson)

FOR ALL the focus on maritime disputes in the South and East China Seas, there is an even greater peril in Asia that deserves attention. It is the rising salience of nuclear weapons in the region. China’s military buildup—in particular its growing capabilities to blunt America’s ability to project effective force in the western Pacific—is threatening to change the military balance in the area. This will lead to a cascade of strategic shifts that will make nuclear weapons more central in both American and Chinese national-security plans, while increasing the danger that other regional states will seek nuclear arsenals of their own. Like it or not, nuclear weapons in Asia are back.

For seventy years, the United States has militarily dominated maritime Asia. During this era, U.S. forces could, generally speaking, defeat any challenger in the waters of the western Pacific or in the skies over them. Washington established this preeminence and has retained it in the high-minded aspirations to foster the growth and development of prosperous, liberal societies within the region. Military primacy has been the crucial underwriter, the predicate of broader American strategy

This primacy is now coming into question. China’s advancing “anti-access/area-denial” (A2/AD) capabilities as well as its expanding strike and power-projection capabilities will present a mounting challenge to the U.S. force posture in the Pacific region—and thus to America’s strategy for the Asia-Pacific as a whole. Beijing appears to be seeking to create a zone in the western Pacific within which the military power of the People’s Liberation Army (PLA) will be able to ensure that Chinese strategic interests are held paramount—in effect, to supplant the United States as the military primate in the region. The oft-cited DF-21D “carrier-killer” ballistic missile is only one small facet of this much broader Chinese effort, which encompasses the fielding of a whole network that integrates a range of increasingly high-quality platforms, weapons, sensors, and command, control and communications systems. Because of this effort, U.S. forces attempting to operate in maritime Asia will now have to struggle for dominance rather than simply assume it.

Indeed, anxiety about the relative military balance between the United States and China is building among the defense officials charged with monitoring it. As Frank Kendall, the Pentagon official with chief responsibility for developing and acquiring new military systems, wrote in a recent paper focused on the implications of China’s military buildup:

While the U.S. still has significant military advantages, U.S. superiority in some key warfare domains is at risk . . . U.S. Navy ships and western Pacific bases are vulnerable to missile strikes from missiles already in the inventory in China . . . The net impact is that China is developing a capability to push our operating areas farther from a potential fight, thereby reducing our offensive and defensive capacity . . . The Chinese are developing an integrated air defense system that puts U.S. air dominance in question, and in some regions, air superiority is challenged by 2020.

Kendall summarized his assessment with the judgment that

China is rapidly modernizing its forces and is developing and fielding strategically chosen capabilities that are designed to defeat power projection capabilities the U.S. depends upon. Technological superiority the U.S. demonstrated over 20 years ago, and which we have relied upon ever since, is being actively challenged.

Nor is Kendall an outlier in this assessment—rather, his view represents something like the evolving baseline understanding among defense officials and experts. Comparably informed and thoughtful defense leaders like Deputy Secretary of Defense Robert Work have said very similar things.

As a result, the United States is beginning to mount an effort to respond to China’s growing capabilities—for instance, through the Defense Department’s recently announced “Offset Strategy” initiative. The Pentagon rightly appears to be focused on maintaining American advantages in the effective projection of conventional military force even in the face of a resolute and highly capable opponent like Beijing. This goal stretches across procurement decisions, revisions to plans and doctrines, changes to deployment and basing, and attitudes toward the exploitation of technology. Outside commentators have tended to conflate this broad effort with the department’s laudable Air-Sea Battle initiative, which is clearly an important segment of the larger attempt to counter challenges to U.S. military superiority, but is still only a part of it. Ideally, this initiative will be successful and will allow the United States to maintain its traditional dominance in maritime Asia. But even if the Pentagon cannot wholly achieve this objective, maintaining even a partial edge in the military balance against China will give the United States valuable deterrent and coercive leverage in what will very likely be a fraught relationship with Beijing.

But achieving even this more modest aspiration is more a hope than a certainty. And the persistence of sequestration, the American political system’s unwillingness to decisively shift resources toward maintaining the military edge in Asia, and the abiding necessity or allure of involvement in other regions raise questions as to how reasonable this hope is. Thus, we cannot be sure how successful the United States will be in retaining its military edge in the region.

In fact, prudence suggests a more pessimistic assessment about the future balance between U.S. and Chinese military strength in the western Pacific. Such moderate pessimism stems not only from domestic political constraints, but also, more importantly, from the assessment that the Chinese economy, even if it slows further (as seems probable), is likely to keep growing significantly—along with the budget for the PLA, which has continued to grow at high levels even as China’s economy has already slowed. And as the Chinese economy continues to mature and advance, we may reasonably expect that the Chinese military will continue to become more technologically sophisticated, professional and capable of effectively conducting what the Chinese refer to as “warfare under informationized conditions”—that is, modern, high-tech war. This will inevitably put pressure on the enormous—and unusual—military advantages that the United States has enjoyed in recent decades.

Accordingly, the future military balance in the western Pacific will, at the very least, be far more even between the United States and China than was previously the case, and likely will become increasingly competitive. Over time, indeed, the balance may tip against the United States and its allies, at least in certain regions and with respect to particular contingencies about which we have traditionally cared. Take Taiwan. Taiwan’s Ministry of National Defense stated in 2013 that the United States would not be able to block a Chinese invasion of the island by 2020. Of course, one might ascribe this judgment to special pleading on the part of Taipei—except that Taiwan’s is not an isolated assessment; many defense experts share this view. Nor should we expect a shift in the balance with respect to Taiwan to be the end of this trend. Rather, if the United States fails to maintain its edge over China, Beijing is likely to be able to attain practical military superiority in areas of maritime Asia other than Taiwan, and over the long term perhaps well beyond it.

SUCH A development would have profound strategic consequences. The United States has seen an open and friendly order in maritime Asia as crucial to its interests at least since Matthew Perry’s “Black Ships” opened Japan in the nineteenth century; since the Second World War, it’s seen its own military supremacy in the Pacific as the best way to secure and promote that order. If China can attain military dominance or even simply advantage in this area, the world’s most dynamic region, then U.S. interests as traditionally understood are likely to suffer, perhaps seriously. It will be Beijing rather than Washington that will serve as the ultimate arbiter of what is and is not acceptable in Asia. It is a reasonable assumption that such a power structure would be considerably less congenial to Washington’s interests—let alone those of U.S. allies—than the current order.

Assuming that the United States will not concede such regional hegemony to Beijing, that the United States and its allies will continue to have significant areas of tension and disagreement with an increasingly capable China, and that the United States will remain ready to use military force to defend or vindicate its and its allies’ interests in Asia, this means that the United States may come to blows with a power deploying military forces of roughly comparable and, in some circumstances, possibly superior effectiveness. In simpler terms, it means that the outcome of a conflict between the United States and China will be more uncertain and that, if current trends are not redressed, the United States might well ultimately find itself on the losing end of a major military engagement in the western Pacific.

This shift toward a more even military balance will lead to significant changes in the Asia-Pacific. It will likely make China more assertive, since Beijing will be more confident that resorting to military force could pay off for it in regional disputes it cares about, especially if a conflict can be kept relatively limited. This point should not be controversial: the notion that greater strength makes one more assertive and ambitious is well demonstrated, both in international politics and in everyday life. China’s rising assertiveness in its near seas in recent years has been fueled by the nation’s general sense of growing power as well as the expanding inventory of assets available to pursue its ambitions. For instance, China’s far more developed maritime and oil-drilling capabilities are playing a major role in Beijing’s increased pushiness in the South China Sea.

War is more likely in situations like this, when both sides think they can prevail, rather than when the prospective winner is clear. The great powers, for example, were more ready to fight in 1914 because each side believed it enjoyed a solid chance of victory. Conversely, a large amount of the stability and comity among the major powers of the post–Cold War world can be traced to a situation of “hegemonic stability”—the evident fact that no other power could venture beyond its own borders to challenge the United States in the years following the 1991 Gulf War. This more stable situation will no longer so clearly hold as resort to force in maritime Asia becomes a more reasonable option for Beijing.

A more even power balance is also likely to lead to a reordering of alignments and strategic postures in the region. Asian and Pacific states will continually judge the relative strength of the two titans of the Asia-Pacific, their resolve and their future trajectories, and adjust their own policies and postures accordingly. Indeed, this is already happening. The old U.S. ally Thailand, for instance, has drifted away from Washington and moved closer to Beijing, while old U.S. adversary Vietnam, feeling the PRC’s pressure in the South China Sea, is warming up to Washington.

THESE FACTORS are becoming increasingly prevalent in discussions of the future of Sino-American relations and of the Asia-Pacific more generally. But one factor that has not been sufficiently appreciated is that the growth of China’s military power vis-à-vis the United States is also very likely to make nuclear weapons grow in salience in the region, and particularly in the Sino-American military balance. More concretely, nuclear weapons may come to loom larger—and perhaps much larger—than they have since the Cold War over U.S. and Chinese military planning, strategic calculations in capitals, and concerns over escalation and brinkmanship in the Asia-Pacific.

This is true for four reasons.

First, a war in the region between the United States and China under circumstances of even rough conventional parity will be more susceptible to nuclear escalation. In the past, most defense analysts and planners envisioned a Sino-American conflict in maritime Asia starting and remaining a conventional fight. Given the PLA’s very modest capabilities for such a contingency, the United States was seen as able to handle any Chinese attempts at power projection solely by relying on U.S. conventional forces and with relatively limited requirements for vertical or horizontal escalation.

In practical terms, the United States would have been able to defeat Chinese attacks on Taiwan or other such plausible beneficiaries of American defense with relatively limited means and on Washington’s terms. Nuclear weapons, if they were to become involved, were seen as most likely to be introduced in limited numbers by the Chinese in a desperate attempt to stave off defeat in a Taiwan contingency, a defeat that might jeopardize the legitimacy of the Communist regime. But the threat to resort to such usage was seen as of limited credibility and actual employment along these lines of minimal effectiveness in light of substantial American advantages in the quality and quantity of the conventional and nuclear forces it could use to conduct such a limited nuclear war.

But we will be moving into a world in which the basic assumptions that determined such assessments no longer hold. That is because future efforts to defeat Chinese attempts at power projection will not be so easily handled, especially without our needing to resort to vertical or horizontal escalation to prevail. In any contingency in the region, the growing sophistication of China’s large military will mean that the United States will have a much more difficult time overcoming it, since Chinese systems that have longer range, are more accurate, are smarter and are more effectively netted together require more work, creativity and skill to defeat. Put more directly, the United States and its allies will have to fight harder, quicker, nastier, deeper, for longer, with less deliberation and over a wider battlefield than was the case in the past in order to defeat Chinese forces in maritime Asia.

For example, in the past, the United States might have designated Chinese fixed ballistic missiles of limited range and accuracy based on or near the coast for attack by aircraft operating safely with excellent and secure information later in a campaign. In the future, however, the United States might have to designate Chinese mobile ballistic missiles of longer range and better accuracy based farther in the country’s interior for attack by aircraft operating perilously with limited information early in a conflict. So, for instance, if Taiwan’s Ministry of National Defense is right that China will have the upper hand in a battle over Taiwan by the 2020s—but the United States still wants to deter or defeat an attempted Chinese invasion of the island—the United States may well need to be willing to hit targets deeper in China than had been envisioned before, strike sooner and expand the war considerably beyond the island’s immediate environs in order to compel Beijing to back away from seizing Taiwan.

Even without anyone really wanting to introduce nuclear weapons into the equation, then, these trends raise classic “inadvertent escalation” risks. This line of analysis points to the dangers of escalation that can arise due to the way even a conventional war can unfold. In particular, if one needs to fight harder against an opponent in order to prevail, it also becomes harder to limit the war—including in ways that might entangle nuclear weapons. For instance, U.S. efforts in the event of conflict to strike at Chinese command-and-control nodes, missile bases and systems, surveillance and intelligence assets, and the like, even if intended only to affect the nonnuclear balance, might well implicate nuclear weapons. This might be because such assets or capabilities might be collocated with nuclear forces or themselves have dual nuclear and conventional roles, because the Chinese might fear such hard-hitting attacks are a prelude to decapitation, or because the Chinese might misread conventional strikes as nuclear attacks. In the fog of war, any number of such dynamics could push toward consideration of nuclear use.

### 2NC – Internal Link – China War

#### Increased China modernization emboldens China and causes a nuclear war – escalates and draws in the U.S.

Cimbala 15 – (Stephen J. Cimbala is Distinguished Professor of Political Science, Penn State Brandywine, an American Studies faculty member and is the author of numerous books and articles in the fields of international security studies, defense policy, nuclear weapons and arms control, intelligence and other fields; Ph.D in political science from Penn State in 1969; “Chinese Military Modernization: Implications for Strategic Nuclear Arms Control,” *Strategic Studies Quarterly*, <http://www.au.af.mil/au/ssq/digital/pdf/Summer_2015/cimbala.pdf>, Accessed 6/29/16, HWilson)

China’s military modernization is going to change the distribution of power in Asia, including the distribution of nuclear and missile forces. This modernization draws not only on indigenous military culture but also on careful analysis of Western and other experiences. As David Lai has noted, “The Chinese way of war places a strong emphasis on the use of strategy, stratagems, and deception. However, the Chinese understand that their approach will not be effective without the backing of hard military power. China’s grand strategy is to take the next 30 years to complete China’s modernization mission, which is expected to turn China into a true great power by that time.”

Chinese military modernization and defense guidance for the use of nuclear and other missile forces hold some important implications for US policy. First, Chinese thinking is apparently quite nuanced about the deterrent and defense uses for nuclear weapons. Despite the accomplishments of modernization thus far, Chinese leaders are aware that their forces are far from nuclear-strategic parity with the United States or Russia. Conversely, China may not aspire to this model of nuclear strategic parity, such as between major nuclear powers, as the key to war avoidance by deterrence or other means. China may prefer to see nuclear weapons as one option among a spectrum of choices available in deterring or fighting wars under exigent conditions and as a means of supporting assertive diplomacy and conventional operations when necessary. Nuclear-strategic parity, as measured by quantitative indicators of relative strength, may be less important to China than the qualitative use of nuclear and other means as part of broader diplomatic-military strategies.

Second, China is expanding its portfolio of military preparedness not only in platforms and weapons but also in the realms of command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) and information technology. Having observed the US success in Operation Desert Storm against Iraq in 1991, Chinese military strategists concluded that the informatization of warfare under all conditions would be a predicate to future deterrence and defense operations.5 As Paul Bracken has noted, the composite effect of China’s developments is to make its military more agile—meaning, more rapidly adaptive and flexible.6 The emphasis on agility instead of brute force reinforces traditional Chinese military thinking. Since Sun Tzu, the acme of skill has been winning without fighting, but if war is unavoidable, delivering the first and decisive blows is essential. This thinking also stipulates that one should attack the enemy’s strategy and his alliances, making maximum use of deception and basing such attacks on superior intelligence and estimation. The combination of improved platforms and command-control and information warfare should provide options for the selective use of precision fire strikes and cyberattacks against priority targets while avoiding mass killing and fruitless attacks on enemy strongholds.

Escalation Control

Another characteristic of the Chinese military modernization that is important for nuclear deterrence and arms control in Asia is the problem of escalation control. Two examples or aspects of this problem might be cited here. First, improving Chinese capabilities for nuclear deterrence and for conventional warfighting increases Chinese leaders’ confidence in their ability to carry out an A2/AD strategy against the United States or another power seeking to block Chinese expansion in Asia. This confidence might be misplaced in the case of the United States. The United States is engaged in a “pivot” in its military-strategic planning and deployment to Asia and, toward that end, is developing US doctrine and supporting force structure for “AirSea Battle” countermeasures against Chinese A2/AD strategy.

Another problem of escalation control is the question of nuclear crisis management between a more muscular China and its Asian neighbors or others. During the Cold War era, Asia was a comparative nuclear weapons backwater, since the attention of US and allied North Atlantic Treaty Organization policy makers and military strategists was focused on the US-Soviet arms race. However, the world of the twenty-first century is very different. Europe, notwithstanding recent contretemps in Ukraine, is a relatively pacified security zone compared to the Middle East or to South and East Asia, and post–Cold War Asia is marked by five nuclear weapons states: Russia, China, India, Pakistan, and North Korea. The possibility of a nuclear weapon use, growing out of a conventional war between India and Pakistan or China and India, is nontrivial, and North Korea poses a continuing uncertainty of two sorts. This latter nation might start a conventional war on the Korean peninsula, or the Kim Jung-un regime might implode, leaving uncertain the command and control over the nation’s armed forces, including nuclear weapons and infrastructure.9

The problem of keeping nuclear-armed states below the threshold of first use or containing escalation afterward was difficult enough to explain within the more simplified Cold War context. Uncertainties would be even more abundant with respect to escalation control in the aftermath of a regional Asian war. There is also the possibility of a US Chinese nuclear incident at sea or a clash over Taiwan escalating into conventional conflict, accompanied by political misunderstanding and the readying of nuclear forces as a measure of deterrence. The point is US and Chinese forces would not actually have to fire nuclear weapons to use them. Nuclear weapons would be involved in the conflict from the outset, as offstage reminders that the two states could stumble into a mutually unintended process of escalation.

An important correction or cautionary note must be introduced at this point. Policy makers and strategists have sometimes talked as if nuclear weapons always serve to dampen escalation instead of exacerbating it. This might be a valid theoretical perspective under normal peacetime conditions. However, once a crisis begins—and especially after shooting has started—the other face of nuclear danger will appear. Thereafter, reassurance based on the assumption that nuclear first use is unthinkable may give way to such an attack becoming very thinkable. As Michael S. Chase has warned, miscalculation in the middle of a crisis is a “particularly troubling possibility,” heightened by uncertainty about messages the sides are sending to one another and/or leaders’ overconfidence in their ability to control escalation.

The “Thucydides Trap” and Nuclear Signaling

Chinese decisions about nuclear force modernization will not take place in a political vacuum. One important issue for US-Chinese strategic planning is whether China and the United States will allow their political relations to fall into the “Thucydides trap,” which refers to the relationship between a currently leading or hegemonic military power and a rising challenger—as in the competition between a dominant Athens and a rising Sparta preceding the Peloponnesian War. The Thucydides trap occurs when a leading and rising power sees their competition as a zero-sum game in which any gain for one side automatically results in a commensurate loss in power or prestige for the other side. It is neither necessary nor obvious that US-Chinese diplomatic-strategic behavior be driven to this end. However, China’s challenges in Asia against US or allied Pacific interests might provoke a regional dispute with the potential to escalate into a more dangerous US-Chinese confrontation, including resort to nuclear deterrence or threats of nuclear first use.

Even if both Washington and Beijing avoid the Thucydides trap, China has the option of using nuclear weapons for diplomatic or strategic objectives short of war or explicit nuclear threats. We miss important possibilities for the political exploitation of nuclear weapons if we confine our analysis of China’s options to threats or acts of nuclear first use or first strike. The following list includes some of the ways China might signal nuclear weapons use to support its foreign policy in possible confrontations with the United States or US Asian allies:

• Nuclear tests during a political crisis or confrontation

• Military maneuvers with nuclear-capable missile submarines or naval surface forces

• Generated alert for air defense forces to reinforce declaration of an expanded air defense identification zone closed to all foreign traffic

• Open acknowledgment of hitherto unannounced—and undetected by foreign intelligence—long- and intermediate-range missiles based underground in tunnels on moveable or mobile launchers

• Adoption of a launch-on-warning policy in case of apparent enemy preparations for nuclear first use

• Cyberattacks against military and critical infrastructure targets in the United States or against a US ally, including important military and command-control networks in Asia, preceded or accompanied by movement of forces to improve first-strike survivability against conventional or nuclear attack

• Relocation of People’s Liberation Army Second Artillery command centers to more protected sites

• Preparation for antisatellite launches against US or other satellites in low earth orbit

• Mobilization of reserves for military units that are nuclear capable • Shake-up of the chain of command for political or military control of nuclear forces or force components

None of the preceding activities would necessarily be accompanied by explicit threats of nuclear first use or retaliation. Chinese political and military leaders would expect US intelligence to notice the actions and hope for US forbearance. China’s expectation might include either a willingness to settle a disagreement based on the status quo or on some newly acceptable terms. Creative analysts or experienced military and intelligence professionals could expand the preceding list; it is neither exhaustive nor definitive of China’s options for nuclear-related signaling.

Contrary to some expert opinion, the relationship between China’s ability to exploit its nuclear arsenal for political or military-deterrent purposes and China’s apparent expertise in cyberwar deserves closer scrutiny. It is true nuclear war and cyberwar inhabit separate universes in terms of organization, mission, and technology. Moreover, the consequences of a nuclear war would certainly be more destructive than any cyberwar fought between the same states or coalitions. In addition, deterrence seems easier to apply as a concept to nuclear war, compared to cyberwar. Among other reasons, the problem of attribution in the case of a nuclear attack is simple compared to the case of a cyberattack.12

Notwithstanding the preceding caveats, in the information age it is likely that cyber and nuclear worlds will have overlapping concerns and some mutually supporting technologies. For the foreseeable future, nuclear-strategic command and control, communications, reconnaissance and surveillance, and warning systems—unlike those of the Cold War—will be dependent upon the fault tolerance and fidelity of information networks, hardware and software, and security firewalls and encryption. Therefore, these systems and their supporting infrastructures are candidate targets in any enemy version of the US Nuclear Response Plan (formerly Single Integrated Operational Plan). In thinking about this nuclear and cyber nexus, it becomes useful to distinguish between a state’s planning for a preventive versus a preemptive attack.

During the Cold War, most of the nuclear-deterrence literature was focused on the problem of nuclear preemption, in which a first-strike nuclear attack would be taken under the assumption that the opponent had already launched its nuclear forces or had made a decision to do so. On the other hand, preventive nuclear war was defined as a premeditated decision by one state to weaken a probable future enemy before that second state could pose an unacceptable threat of attack. Most Cold War political leaders and their military advisors rightly regarded preventive nuclear war as an ethically unacceptable and strategically dysfunctional option.13

In a world in which the day-to-day functioning of military forces and civil society is now dependent upon the Internet and connectivity, the option of a preventive war with two phases now presents itself to nuclear-armed states. In the first phase, selective cyberattacks might disable key parts of the opponent’s nuclear response program—especially nuclear-related C4ISR. In the second phase, a nuclear threat of first use or first strike might follow against an enemy partially crippled in its ability to analyze its response options or to order those responses into prompt effect. If this scenario seems improbable in the context of large states like the United States, Russia, and China because of their force and command-control diversity and protection, consider how it might work in the context of confrontations between smaller nuclear armed states, including hypothetical future India-Pakistan or Israel-Iran showdowns.14 Even in the cases of US conflict with China or Russia (or between China and Russia), nuclear crisis management would certainly include preparation for possible cyber attacks preceding or accompanying nuclear first use or first strike.

### 2NC – AT: No Escalation

#### US-China war goes nuclear and escalates

Colby 14 – (Elbridge Colby is the Robert M. Gates Fellow at the Center for a New American Security, 12/19/14, “Welcome to China and America's Nuclear Nightmare,” *National Interest*, <http://nationalinterest.org/feature/welcome-china-americas-nuclear-nightmare-11891?page=show>, Accessed 6/27/16, HWilson)

Many critics of Air-Sea Battle, like the National Defense University’s T. X. Hammes, build their case on these concerns. They argue that the risks of such escalation are simply too great to justify a defense posture against China that includes plans for strikes on the mainland. These critics are right that the problems posed by inadvertent escalation are very real and demand attention, but they are wrong to contend that the United States should dispense with a powerful strike posture against China because of it. Quite the contrary. Such a posture is essential if the United States is to maintain an effective conventional deterrent in the western Pacific and thus is necessary if Washington is to continue to pursue its long-standing strategy toward the region. And such a posture can be structured and the plans for how it would be used in war designed and implemented in ways that mitigate the risks of escalation.

But while limited war is possible under the nuclear shadow, it is neither easy nor a sure thing. Accordingly, it should be a major focus of defense officials and planners to pay greater attention to the serious challenges of structuring a conventional war plan such that it does not encourage nuclear escalation on the part of the adversary. More broadly, U.S. and Chinese leaders should bear in mind that controlling a war, even one that both seek to keep conventional, might be exceedingly difficult; the control of escalation between nuclear-armed adversaries is inherently more a stochastic than a determinate process. That said, such caution cannot be allowed to lead to passivity or acquiescence on the part of Washington in its work to strengthen its conventional posture in the Pacific. Rather, it must lead to a vigorous fortifying of the U.S. position, along with the greatest rigor in structuring American war plans and forces to mitigate these risks—and the greatest prudence in employing any such plans.

A SECOND reason why nuclear weapons are likely to become more salient in the Sino-American military balance is because China’s nuclear arsenal is becoming somewhat larger and considerably more sophisticated. While China continues to exhibit restraint regarding the size of its nuclear arsenal and in how it appears to think about the role of nuclear weapons in its military strategy, the PRC is nevertheless substantially modernizing its nuclear forces. These improvements include the deployment of more survivable road-mobile intercontinental ballistic missiles armed with multiple, independently targetable warheads and penetration aids designed to defeat missile defenses; the development and gradual deployment of a ballistic-missile submarine force; the fielding of new command, control and communications assets that enable more deliberate and controlled employment; and the marked improvement in training and professionalism among the PLA’s nuclear warriors. The Department of Defense conservatively judged in its 2014 annual report to Congress on China’s military modernization that “these technologies and training enhancements strengthen China’s nuclear force and enhance its strategic strike capabilities” and assessed that China will “implement more sophisticated command and control systems.”

Whether deliberately pursued or not, these improvements will by necessity give Beijing more and better options for employing its nuclear weapons, especially in more limited and controlled ways. In the past, China’s nuclear forces were considered vulnerable and blunt instruments, messy weapons that would only likely be used at the very top of the “escalatory ladder”—for instance, against the cities of its opponents. Needless to say, this presumably rendered the bar for Chinese nuclear use exceptionally high, an inference fortified by China’s oft-trumpeted (if ambiguous and rarely fully trusted) “no first use” policy regarding its nuclear weapons.

But, armed with its new generation of nuclear forces, China will gain options for using them that are more discriminate in nature than those entailing massive strikes against American territory. Instead of only, practically speaking, having the option of striking at a major American or Japanese city, China will increasingly gain the ability to employ its nuclear forces in more tailored fashion—for example, against military facilities or forces, including in the region. This ability to use nuclear weapons in more limited and tailored ways will make China’s threats—explicit or implicit—to use nuclear forces more credible.

The consequence of this is that China’s nuclear force will cast a darker shadow over Sino-American competition in the Pacific. Thus, strategists and military planners in the United States and allied countries will need to take the possibility of Chinese nuclear employment in the event of conflict more seriously. This does not mean that China will reach for the nuclear saber early or often. But a more sophisticated force will give China better options for how it might seek to use these weapons not only, as in the past, as a desperate last resort, but also to deter U.S. escalation of a conflict—escalation the United States might need to resort to if it is to prevail.

THIS RAISES the third reason why nuclear weapons are likely to become more relevant in the Asia-Pacific. This stems from the unfortunate fact that the United States may lose the conventional military advantage it has historically enjoyed over China in maritime Asia. Such a loss would most plausibly be partial—China would be unlikely to seize whole the conventional upper hand in the region. But, having gained the advantage over some parts of the western Pacific, Beijing might, for example, attempt to force the United States into a situation in which Washington would be unwilling to take the necessarily escalatory steps to overcome or push back Chinese attacks. For instance, Beijing might gain conventional superiority around Taiwan and be able to block U.S. efforts designed to defend the island. In such a case, the United States might need to broaden the war, possibly by striking targets further into China and of greater value to the PRC’s leadership, in order to persuade Beijing to agree to acceptable terms. The plausible threat of a limited Chinese nuclear response would prove a substantial disincentive to pursuing such a course.

A loss of U.S. conventional advantages in maritime Asia could come about because of a U.S. lack of resolve or inattention, because of the scale and effectiveness of China’s substantial and ongoing military buildup, or because of some malign combination of both. Such a shift in the balance is more plausible in the foreseeable future regarding the western portions of the Pacific, but this apparent narrowing of the problem actually offers little comfort since the western Pacific is home to Japan, South Korea, Taiwan and the nations of Southeast Asia, and is the eastern gateway to the Indian Ocean and the Persian Gulf. Losing military primacy and thus regional strategic leadership there is hardly compensated for by preserving it over the Samoan Islands. Moreover, military primacy lost in the western Pacific is just as likely to be simply a stage on the way to further erosion as it is to be the terminus of a shift in the military balance.

In the event that the United States does lose its conventional advantage, Washington may well seek to rely on its own nuclear weapons to compensate for outright inferiority or for the inability of its conventional forces to fight back in a way sufficiently controlled to suit U.S. interests in limiting a conflict. This reliance would, in effect, be a return to U.S. policy during the Cold War, when Washington relied on its nuclear forces to offset Soviet conventional superiority in Europe. In particular, Washington would likely seek to exploit its superior ability to conduct a limited nuclear war to deter China from taking advantage of its conventional lead.

Nor would this be likely to be a unilateral move on the part of the United States. Rather, it is reasonable to expect that beneficiaries of U.S. security guarantees would press for Washington’s clearer and more emphatic adoption of such an approach. Even in a far more congenial security environment than the future sketched here, U.S. allies like Japan, South Korea and Australia have been insistent that the United States reaffirm that Washington’s security guarantee ultimately is rooted in its commitment to use nuclear weapons to defend them. If the Chinese are able to develop not only the A2/AD capabilities but also the strike and power-projection assets needed to overcome U.S. conventional superiority, it seems reasonable to expect that U.S. allies will urge Washington to substitute for that conventional deficit with the nuclear force they already see as vital to their security.

THIS COURSE will seem unappealing to many, not least in the United States, given the risks it will entail for Americans. But this disquiet points to the fourth and final reason why nuclear weapons are likely to become more salient in the Asia-Pacific: the prospect of further nuclear proliferation in the region. If, as China grows stronger and more assertive, its conventional military power begins to outweigh that of the United States in maritime Asia, and that shift is not met by a greater U.S. reliance on its nuclear forces or some other effective countervailing steps, then those countries of Asia traditionally allied to Washington—countries that cannot hope to match China’s strength at the conventional level—may ultimately see getting their own nuclear weapons as essential to deterring China’s exploitation of its growing strength.

It is worth emphasizing that this will particularly be the case if these nations view a weaker United States as lacking the resolve or the ability to use its nuclear weapons on behalf of its allies, since in such a case they will be exposed to Chinese coercion. This is no fantasy; polls in South Korea already show substantial support for an indigenous nuclear-weapons program, and South Korea, Japan, Australia and Taiwan have seriously contemplated pursuing their own nuclear arsenals in the past and might do so again. In other words, in such a scenario a cruel dynamic will take hold in which diminishing U.S. conventional advantages will lead to pressure for greater emphasis on nuclear forces, but, in light of China’s own advancing nuclear capabilities, such reliance itself will be decidedly less attractive.

### 2NC – Impact – Regional Heg

#### China displacing the US as the regional hegemon causes regional instability

Pollmann 16 – (Mina Erika Pollmann is a senior in the Edmund A. Walsh School of Foreign Service majoring in International Politics with a concentration in Foreign Policy and the Ellsworth Bunker Undergraduate Fellow; She is an Honors Candidate and participant of the Georgetown-Japan 2020 Initiative. Her research interests focus on Japan's security and regional diplomacy; 6/23/16, “Experts Imagine an Asia Without the US,” <http://thediplomat.com/2016/06/experts-imagine-an-asia-without-the-us/>, Accessed 6/29/16, HWilson)

A panel of Asia experts recently conveyed to American audiences the alarm that Asian observers feel about U.S. withdrawal from the region. Gathering in New York on Monday for a panel hosted by NTT and Kinokuniya — a Japanese publishing company and book store, respectively – the experts discussed a wide range of divisive issues in Asia’s security landscape – from the Korean peninsula to the East and South China Seas. Despite covering Asian power politics from different geographical lenses, all the speakers agreed on the importance of U.S. commitment to maintaining a stable balance of power in Asia, especially in light of China’s reemergence as a major player.

Chisako Masuo, an associate professor at the Graduate School of Social and Cultural Studies at Kyushu University, warned that “the Asian power balance is more vulnerable than Americans believe.” Because of concerns about U.S. withdrawal, Asian countries are preparing for the worse case scenario: An Asian regional order without U.S. leadership would not be a rules-based order, but a China-based order. Other Asian countries wouldn’t be happy with that development, but they would have no choice but to go along if the United States will not help provide balance, Masuo explained. In this sense, the U.S.-Japan alliance is an “important pillar” to maintain an open, liberal, rules-based order in Asia.

This is not containment of China, Masuo was quick to point out. If the game board is transparent and fair, China can play a mutually beneficial game with other Asian countries. One example Masuo highlights is how the creation of the Asian Infrastructure Investment Bank (AIIB) spurred the Asian Development Bank (ADB) to do better. But, she adds, such friendly competition requires a “quiet U.S. military presence” in the background. And despite a much-touted “rebalance to Asia,” experts on the panel remain unconvinced of U.S. commitment to the region.

“In dealing with China … not only Japan, but Vietnam and the Philippines, in a way, were all disappointed about Obama’s actions towards [China] reclaiming islands [in the South China Sea]. He sent naval vessels only three times so far, and it’s just too weak,” Masuo lamented. “And if Trump was going to succeed him, maybe [Trump wouldn’t] do anything, but then, this Asian power balance is gone.”

This sentiment is echoed by Kan Kimura, a professor at Kobe University’s Graduate School of International Cooperation Studies, who explains, “American people have to understand how [strongly Asian peoples fear the] withdrawal of U.S. troops.”

For reassuring nervous Asian partners, U.S. commitment isn’t enough — U.S. messaging is also important. This is easier said than done, of course. Putting aside the isolationist sentiment that the bombastic presumptive Republican nominee Donald Trump has resurrected during this campaign season, even official Obama administration messaging can be received, or interpreted, differently based on any given audience states’ own preoccupations. In geopolitics, a country’s placement in a particular geographic circumstance will shape their assessment of potential threats and other countries’ intentions.

Kimura expanded on this concept to explain why Japan and South Korea have such different perceptions of the tenor of U.S.-China relations. As a maritime power, the United States has expected more from Japan, demanding that Japan play a larger role in recent disputes in the East and South China Seas. Because of this, Japan has seen the more hard-line elements of U.S. China policy, leading to expectations that the United States will be around to stand up to China for decades.

Meanwhile, as a land power, South Korea has not had to deal with the same sort of U.S. expectations and has mostly sat out the disputes in the East and South China Seas. Not having seen the hard-line elements that Japan interacts with, South Korea expects the United States to take a softer policy tack, and believes Washington will give them a “hall pass” when it comes to leaning on China. The challenge for the United States, Kimura concluded, is to send a clearer message to Asian countries. It’s a typical Goldilocks dilemma: while Japan overestimates how hard-line U.S. China policy will be, South Korea underestimates it.

There is some strength to the argument that ambiguity serves U.S. interests, however. As Kimura noted, from the U.S. perspective, a clear commitment could raise concerns about moral hazard; countries such as the Philippines might be willing to take unnecessary risks if they believe Washington will have their back.

Amid all this concern about the strength of U.S. commitment, there is a bright spot, as Tuong Vu, a political science professor at University of Oregon, points out: “the Trans-Pacific Partnership (TPP) is a good example of the U.S.’s biggest efforts to involve Vietnam, to help Vietnam deal with the Chinese threat.”

While in popular discourse the military dimension of the American rebalance might have gotten the most attention, it is really this economic dimension that underpins why the United States – for its own interest – should stay committed to Asia. Responding to questions about why the U.S. ought to care about Asia and its thorny maritime issues, Masuo rebutted: “But think about it, Asia is the center of economic development. And if the U.S. chooses not to establish stronger relations with Asia, how is it going to maintain prosperity for its own people?”

#### Asian instability causes conflicts that go nuclear and tank the global economy

Tan, Associate Professor, School of Social Sciences – University of New South Wales, ‘15

(Andrew T.H., “The prospects for conflict in East Asia”, *Security and Conflict in East Asia*, Routledge International Handbooks)

High tensions in East Asia

The high tensions in East Asia, the highest since the end of the Second World War, have led to fears of open conflict involving the states in the region as well as extra-regional powers, in particular the USA, By early 2013, tensions between North Korea on the one hand, and South Korea, the USA and Japan, on the other, had deteriorated to their worst level since the end of the Korean War in 1953, sparking fears of an **accidental war** due to North Korea’s brinkmanship and political miscalculation (ICG 2013a). Tensions between the People’s Republic of China and Japan were also at their highest since the end of the Second World War, due to their dispute over the Diaoyu/Senkaku Islands (Hughes 2013). More seriously, China, the USA and North Korea possess nuclear weapons, and Japan has always been regarded as a threshold nuclear power, as it possesses plutonium stocks generated through its power industry, ballistic missile capability and the technology to rapidly transform itself into a significant nuclear weapons power should it choose to do so (Rublee 2010: 62-63). South Korea could also be forced to develop its own nuclear weapons if the threat from a hostile, aggressive and unpredictable North Korea continues to grow as it develops its nuclear, chemical and biological weapons capabilities, and uses them to coerce South Korea (New York Times 2013).

The impact of any regional conflict in East Asia will be **significant and global**. Any conflict in this region would involve not only states in the region and US allies from further afield, but also **quickly escalate into a** nuclear conflict, given the superiority that the USA enjoys in terms of conventional warfare capabilities over North Korea, and to a diminishing degree, China, thus forcing them to resort to non-conventional means, such as nuclear weapons, in any major conflict. Indeed, the US strategy of Air-Sea Battle, which involves attacking China’s surveillance, intelligence and command systems, are likely to be interpreted by China as attempts to disarm its nuclear strike capability and could thus lead to a quick arid unwanted escalation into a nuclear conflict (Schreer 2013).

Moreover, today the **centre of the global economy** no longer resides in Europe or North America but in Asia, in particular, East Asia. Indeed, three of the key actors in the region, namely the USA, China and Japan, are also the three largest economies in the world, with South Korea ranked 15th in global terms, according to the World Bank. Any conflict in East Asia will therefore have a **profound, global economic impact**. Furthermore, the fact that **any conflict could escalate into** a major war, including **nuclear war**, means that conflict in East Asia will have global implications as well as uncertain consequences for the international system.

### 2NC – Impact – Asia Prolif

#### Asia prolif causes nuclear war

Cimbala 15 – Stephen J. Cimbala, Distinguished Professor of Political Science at Pennsylvania State University Brandywine, The New Nuclear Disorder: Challenges to Deterrence and Strategy, 2015, pp. 59-63

The spread of nuclear weapons in Asia (including those parts of the Middle East with geostrategic proximity or reach into Asia) presents a complicated mosaic of possibilities in this regard. States with nuclear forces of variable force structure, operational experience, and command-control systems will be thrown into a matrix of complex political, social and cultural cross-currents contributory to the possibility of war. In addition to the existing nuclear powers in Asia, others may seek nuclear weapons if they feel threatened by regional rivals or hostile alliances. Containment of nuclear proliferation in Asia is a desirable political objective for all of the obvious reasons. Nevertheless, the present century is unlikely to see the nuclear hesitancy or risk aversion that marked the Cold War: in part, because the military and political discipline imposed by the Cold War superpowers no longer exists, but also because states in Asia have new aspirations for regional or global respect.20¶ The spread of ballistic missiles and other nuclear capable delivery systems in Asia, or in the Middle East with reach into Asia, is especially dangerous because plausible adversaries live close together and are already engaged in ongoing disputes about territory or other issues. The Cold War Americans and Soviets required missiles and airborne delivery systems of intercontinental range to strike at one another’s vitals. But short range ballistic missiles or fighter-bombers suffice for India and Pakistan to launch attacks at one another with potentially “strategic” effects. China shares borders with Russia, North Korea, India and Pakistan; Russia, with China and North Korea; India, with Pakistan and China; Pakistan, with India and China; and so on.The short flight times of ballistic missiles between the cities or military forces of contiguous states means that very little time will be available for warning and attack assessment by the defender. Conventionally armed missiles could easily be mistaken for a tactical nuclear first use. Fighter-bombers appearing over the horizon could just as easily be carrying nuclear weapons as conventional ordnance. In addition to the challenges posed by shorter flight times and uncertain weapons loads, potential victims of nuclear attack in Asia may also have first strike vulnerable forces and command-control systems that increase decision pressures for rapid, and possibly mistaken, retaliation. This potpourri of possibilities challenges conventional wisdom about nuclear deterrence and proliferation on the part of policy makers and academic theorists. For policy makers in the United States and NATO, spreading nuclear and other weapons of mass destruction in Asia could profoundly shift the geopolitics of mass destruction from a European center of gravity (in the twentieth century) to an Asian and/or Middle Eastern center of gravity (in the present century).21 This would profoundly shake up prognostications to the effect that wars of mass destruction are now passé, on account of the emergence of the “Revolution in Military Affairs” and its encouragement of information-based warfare.22 Together with this, there has emerged the argument that large scale war between states or coalitions of states, as opposed to varieties of unconventional warfare and failed states, are exceptional and potentially obsolete.23 The spread of WMD and ballistic missiles in Asia could overturn these expectations for the obsolescence or marginalization of major interstate warfare.

### 2NC – AT: No Asia Prolif

#### Yes Asia prolif – tech exists, 6 states are at break-out, and deterrence fails

Sempa 16 – (Francis P. Sempa is the author of Geopolitics: From the Cold War to the 21st Century (Transaction Books) and America’s Global Role: Essays and Reviews on National Security, Geopolitics and War (University Press of America). He is also a contributor to Population Decline and the Remaking of Great Power Politics (Potomac Books). He has written on historical and foreign policy topics for Joint Force Quarterly, American Diplomacy, the University Bookman, The Claremont Review of Books, The Diplomat, Strategic Review, the Washington Times and other publications. He is an attorney, an adjunct professor of political science at Wilkes University, and a contributing editor to American Diplomacy; 2/7/16, “Nuclear Instability in the Asia-Pacific Region?,” *The Diplomat*, <http://thediplomat.com/2016/02/nuclear-instability-in-the-asia-pacific-region/>, Accessed 6/28/16, HWilson)

Henry D. Sokolski, the executive director of the Nonproliferation Policy Education Center and former Pentagon official and consultant to the Office of Net Assessment, has written a thoughtful and sobering study on the potential for nuclear proliferation and competition in the Asia-Pacific region. Published in January 2016 by the U.S. Army War College Press, Underestimated: Our Not So Peaceful Nuclear Future, presents a bleak but not altogether hopeless view of current trends in the development of strategic, intermediate and battlefield nuclear weapons, the spread of ballistic missile technology, and the proliferation of nuclear weapons-grade material throughout the region.

This vision is not shared by most of the world’s policymakers and academic theorists who instead see the world becoming a safer place as the United States and Russia continue to reduce their stockpiles of nuclear weapons, nuclear deterrence becomes virtually “automatic,” and non-nuclear powers obtain “peaceful” nuclear facilities and materials. Sokolski argues that the more sanguine views of the nuclear future in the Asia-Pacific fail to “fully explore the regional insecurities that arise with threatened nuclear weapons breakouts or ramp-ups,” ignore the “significant overlaps between civilian and military nuclear activities or the risk that ‘peaceful’ nuclear facilities or materials might be diverted to make bombs,” and downplay the potential strategic instability that may result from U.S.-Russian nuclear disarmament in the face of nuclear weapons build-ups by China, India, Pakistan, and possibly other regional states, and the proliferation of nuclear facilities and materials.

If current trends continue, Sokolski explains, “[t]he strategic military competitions of the next . . . decades will be unlike any the world has yet seen.” At the height of the Cold War, the nuclear arsenals of the United States and Soviet Union dwarfed those of the world’s other nuclear powers. Today, while the U.S. and Russia freeze or continue to reduce their nuclear arsenals, China, India, and Pakistan are increasing and modernizing their strategic nuclear forces; which means that “the next arms race will be run by a much larger number of contestants with highly destructive strategic capabilities far more closely matched and capable of being quickly enlarged than in any other previous period in history.”

According to Sokolski, Russia currently fields 3600 strategic and tactical nuclear weapons, the U.S. has 2130, China has somewhere between 190 and 900, while India, Pakistan, England, France and Israel each field between 100 and 400. “[T]he difference in the numbers of nuclear deployments between the top and bottom nuclear powers. . .,” he writes, “has fallen at least two full orders of magnitude and is projected to decline even further.” Moreover, because of the spread of weapons-grade material and nuclear facilities, at least six other countries – Iran, Saudi Arabia, South Korea, Japan and Algeria – are considered “possible near-or mid-term nuclear weapons-ready states.” This means, writes Sokolski, that “the stool of nuclear deterrence will have many more legs that could give way in many more surprising ways than were possible a half-century ago.”

Other developments in this area provide additional reasons for concern. Russia and Pakistan have doctrinally indicated that they will use nuclear weapons first against opponents’ conventional forces. China is reconsidering its declared “no first use” policy. Russia, China, and North Korea have constructed or expanded underground nuclear complexes to both hide and protect nuclear forces. Twenty-four nations have acquired ballistic missile systems capable of delivering nuclear warheads.

Although much has been written about China’s rise as a global power and potential peer competitor to the United States, less attention has been paid to China’s growing nuclear arsenal and capabilities. Sokolski notes China’s efforts to modernize its nuclear-capable missiles; its production of sufficient weapons-grade plutonium and uranium to make as many as 1200 nuclear weapons; its development and deployment of ballistic missile submarines; its construction and deployment of the DF-41 ICBM; its deployment of multiple independently targetable warheads (MIRVs) on the DF-5 missiles; and its increased uranium enrichment capacity, which will enable China to build more than five hundred nuclear weapons per year by the year 2020. These trends threaten to undermine the effectiveness of the U.S. extended nuclear umbrella to Japan and South Korea, and cast doubts on America’s ability to protect Taiwan, the Philippines, Australia, and other allies in the region. That, in turn, could lead Japan and South Korea, and perhaps other vulnerable countries, to seek their own nuclear deterrent. “These trends,” Sokolski writes, “invite disorder. How much depends on how well the United States, Russia, China, and other key states deal with them.”

### 2NC – Impact – Economy

#### Corporate espionage causes economic decline – perception of CFIUS ineffectiveness is sufficient to trigger the link

Lukas 13 – (Carrie L. Lewis is a graduate of Princeton University and Harvard's Kennedy School of Government; currently is the managing director of the Independent Women's Forum, writes for Forbes, and is the vice president for policy and economics at the Independent Women's Voice; 6/4/13, “It's Time for the U.S. to Deal with Cyber-Espionage,” <http://www.usnews.com/opinion/articles/2013/06/04/chinas-industrial-cyberespionage-harms-the-us-economy>, Accessed 6/28/16, HWilson)

Cyberwarfare and corporate espionage sound like the basis of a good summer beach read: the perfect escape from the too-gloomy realities of an economy that continues to sputter, leaving millions of Americans out of work and millions more underemployed. Yet Americans should be aware that far from fiction, industrial espionage has become a common occurrence and one that adds heavily to our economic woes.

The numbers involved are staggering. The director of the National Security Agency, Gen. Keith Alexander, called cybercrime "the greatest transfer of wealth in history." The price tag for intellectual property theft from U.S. companies is at least $250 billion a year. That's far more than what businesses pay in federal corporate income taxes.

Imagine what recouping those lost billions would mean to our economy and American workers: More jobs, higher pay, and lower prices would be the immediate result. It would also mean more innovation and a higher standard of living in the future. Today, business leaders have reason to be reluctant to invest scarce resources on research and development since that information and innovation may be stolen before they can bring new products to market. Without the specter of this crime, more money would be invested in identifying new technologies and medical breakthroughs that would make our lives healthier and richer.

Of course, there is no way that America can identify, let alone stop, every cyberhacker. Yet cyber-espionage isn't primarily just the work of entrepreneurial, tech-savvy criminals. Much of the dirty work is done by state-sponsored cyberspies, who are purposefully draining information from vital U.S. infrastructure systems and businesses.

The Virginia-based cyber security firm Mandiant recently released a report detailing one source of persistent cyber attacks, the Chinese People's Liberation Army. Mandiant estimates that since 2006, a single Chinese army cyberattack unit has compromised "141 companies spanning 20 major industries, from information technology and telecommunications to aerospace and energy," using a "well-defined attack methodology, honed over years and designed to steal large volumes of valuable intellectual property."

Mandiant explains that once these hackers have infiltrated an organization's system, they "periodically revisit the victim's network ... and steal broad categories of intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and emails and contact lists". On average, access to a victimized network is maintained for nearly a year.

Unsurprisingly, it's not just businesses that are hemorrhaging proprietary information and losing vast amounts of wealth as a result of these attacks. The United States government is a frequent victim, and national security, rather than just dollars, is often a casualty.

The General Accounting Office found that in 2012 federal agencies reported 46,562 cyber security incidents. That's a big uptick from 5,503 incidents in 2006. GAO concludes that such attacks "have placed sensitive information at risk, with potentially serious impacts on federal and military operation; critical infrastructure; and confidentiality, integrity, and availability of sensitive government, private sector, and personal information." GAO also details how federal agencies across the board have been insufficient in creating plans to deter, detect and address such cyber threats.

#### Economic decline causes global war

Royal 10 (Jedediah, Director of Cooperative Threat Reduction – U.S. Department of Defense, “Economic Integration, Economic Signaling and the Problem of Economic Crises”, Economics of War and Peace: Economic, Legal and Political Perspectives, Ed. Goldsmith and Brauer, p. 213-215)

Less intuitive is how periods ofeconomic decline may increase the likelihood of external conflict. Political science literature has contributed a moderate degree of attention to the impact of economic decline and the security and defence behaviour of interdependent states. Research in this vein has been considered at systemic, dyadic and national levels. Several notable contributions follow. First, on the systemic level, Pollins (2008) advances Modelski and Thompson's (1996) work on leadership cycle theory, finding thatrhythms in the global economy are associated with the rise and fall of a pre-eminent power and theoften bloody transition from one pre-eminent leader to the next. As such, exogenous shocks such aseconomic crises could usher in a redistribution of relative power(see also Gilpin. 1981) that leads to uncertainty about power balances,increasing the risk of miscalculation **(**Feaver, 1995). Alternatively,even a relatively certain redistribution of power could lead to a permissive environment for conflictas a rising power may seek to challenge a declining power (Werner. 1999). Separately, Pollins (1996) also shows that global economic cycles combined with parallel leadership cycles impact the likelihood of conflict among major, medium and small powers, although he suggests that the causes and connections between global economic conditions and security conditions remain unknown. Second, on a dyadic level, Copeland's (1996, 2000) theory of trade expectations suggests that **'**future expectation of trade' is asignificant variable in understanding economic conditions and security behaviour of states**.** He argues that interdependent states are likely to gain pacific benefits from trade so long as they have an optimistic view of future trade relations. However,if the expectations of future trade decline**,** particularly for difficult to replace items such as energy resources,the likelihood for conflict increases, as states will be inclined to use force to gain access to those resources. Crises couldpotentially be thetriggerfor decreased trade expectationseither on its own or because it triggers protectionist moves by interdependent states.4 Third,others have considered the link between economic decline and external armed conflict at a national level. Blomberg and Hess(2002)find a strong correlation between internal conflict and external conflict, particularly duringperiods ofeconomic downturn. They write: The linkages between internal and external conflict and prosperity are strong and mutually reinforcing. Economic conflict tends to spawn internal conflict, which in turn returns the favour. Moreover, thepresence of a recession tends to amplify the extent to which international and external conflicts self-reinforce each other**. (**Blomberg & Hess, 2002. p. 89)Economic decline hasalsobeen linked with an increase in the likelihood of terrorism **(**Blomberg, Hess, & Weerapana, 2004), which has the capacity to spill across borders and lead to external tensions. Furthermore, crises generally reduce the popularity of a sitting government."Diversionary theory" suggests **that,** when facing unpopularity arising from economic decline, sittinggovernments have increased incentives to fabricate external military conflicts to create a 'rally around the flag'effect**.** Wang (1996), DeRouen (1995). and Blomberg, Hess, and Thacker (2006) find supporting evidence showing that economic decline and use of force are at least indirectly correlated. Gelpi (1997), Miller (1999), and Kisangani and Pickering (2009) suggest thatthe tendency towards diversionary tactics are greater for democratic statesthan autocratic states, due to the fact that democratic leaders are generally more susceptible to being removed from office dueto lack of domestic support. DeRouen (2000) has provided evidence showing thatperiods of weak economic performance in the UnitedStates, and thus weak Presidential popularity, are statistically linked to an increase in the use of force. In summary, recent economic scholarship positively correlates economic integration with an increase in the frequency of economic crises, whereas political science scholarship links economic decline with external conflictat systemic, dyadic and national levels.5 This implied connection between integration, crises and armed conflict has not featured prominently in the economic-security debate and deserves more attention.

### ---XT: Espionage Hurts Econ

#### China’s the biggest espionage threat to the US – tanks the economy

Dean 15 – (Matt Dean is the Department of Justice & federal law enforcement producer for Fox News Channel; 7/25/15, “FBI: China the most predominant economic espionage threat to US,” *Fox News*, <http://www.foxnews.com/politics/2015/07/25/fbi-china-most-predominant-economic-espionage-threat-to-us.html>, Accessed 6/29/16, HWilson)

Spies, largely of Chinese origin, are going to dramatic lengths to steal critical information from U.S. companies, officials within the intelligence community say.

The Federal Bureau of Investigation on Thursday detailed a sharp spike in the number of economic espionage investigations undertaken by the agency over the last year, with a 53 percent increase in caseloads.

Randall Coleman, the head of the agency’s counterintelligence division, said in a briefing that state-sanctioned corporate theft by China is at the core of the problem.

Coleman said that Beijing is the most predominant threat facing the United States from the standpoint of economic espionage.

The federal government’s data appears to show just how deep this problem runs.

A recent FBI survey of 165 U.S. companies found that China was the perpetrator in 95 percent of economic-espionage cases.

Officials say that theft of trade secrets and intellectual property has resulted in the loss of hundreds billions of dollars from the U.S. economy over the last year alone.

Other big targets for economic spies are specifications for U.S. military technology and proprietary information on everything from superconductors to seed-and-grain hybrids.

“It’s across the board,” said Dean Chappell, a section chief in the FBI’s counterintelligence division. “It’s not high-end avionics for military aircraft; it’s not joint strike fighter stuff. It’s all of the things that we see every day.”

In a change from more traditional modes of economic espionage, such spies are appearing as non-traditional actors, serving as insider threats within organizations and institutions, officials say.

William Evanina, head of the National Counterintelligence and Security Center, said such individuals have been observed in the U.S. serving as professors, engineers, travelling students and businessmen.

Officials also warn of cyber tactics used to hijack intellectual property and trade secrets.

In particular, actors, predominantly from China, are known to employ mass spear-phishing campaigns to coax employees inside companies into clicking tainted links or attachments.

If successful, the actor could get critical data off of the organization’s computer network.

China in particular has been publicly outed on multiple occasions by the Obama administration for its efforts geared toward breaching private sector interest.

U.S. economists blame Beijing for contributing to an increasingly uneven playing field on the world economic scene.

“To sustain its phenomenal growth rate, China must employ cyberattacks to steal information,” said Scott Borg, director and chief economist of U.S. Cyber Consequences Unit, a non-profit research institute. “Cyberattacks stealing competitively important business information are a fundamental part of the national economic development strategy of China. For this reason, getting China to moderate this behavior will be extremely difficult.”

As a result, The FBI has announced a nationwide awareness campaign and continues to develop relationships within U.S. industry.

The agency, for example, assigns agents to serve as strategic partnership coordinators with companies that may have been the victim of intellectual property or trade secret theft.

The coordinators are stationed at each of the agency’s 56 field offices.

The campaign has also prompted the FBI to take a visual approach in spreading its message.

“The Company Man: Protecting America’s Secrets” is a highly produced short video commissioned by the agency that depicts a real-life case of economic espionage handled by the feds.

The agency has shown it in 1,300 briefings with companies across the nation in hopes of raising awareness on the issue.

“Protection of our proprietary information and trade secrets is a critical pillar to our national security,” Evanina said. “The way we look at it, economic security is national security.”

#### Chinese economic espionage hits thousands of companies and tanks the economy

Stahl 16 – (Lesley Rene Stahl is an American television journalist. She has spent most of her career with CBS News, having been affiliated with that network since 1972; since 1991, she has reported for CBS' 60 Minutes; the article cites interviews with her and John Carlin, assistant attorney general for National Security with responsibility for counterterrorism, cyberattacks and increasingly economic espionage, Daniel McGahn, the head of American Superconductor, and Dmitri Alperovitch and George Kurtz, cofounders of a computer security firm called CrowdStrike; 1/17/16, “The Great Brain Robbery,” *CBS News: 60 Minutes*, <http://www.cbsnews.com/news/60-minutes-great-brain-robbery-china-cyber-espionage/>, Accessed 6/30/16, HWilson)

Economic espionage sponsored by the Chinese government is costing U.S. corporations hundreds of billions of dollars and more than two million jobs

If spying is the world's second oldest profession, the government of China has given it a new, modern-day twist, enlisting an army of spies not to steal military secrets but the trade secrets and intellectual property of American companies. It's being called "the great brain robbery of America."

The Justice Department says that the scale of China's corporate espionage is so vast it constitutes a national security emergency, with China targeting virtually every sector of the U.S. economy, and costing American companies hundreds of billions of dollars in losses -- and more than two million jobs.

John Carlin: They're targeting our private companies. And it's not a fair fight. A private company can't compete against the resources of the second largest economy in the world.

John Carlin is the assistant attorney general for National Security with responsibility for counterterrorism, cyberattacks and increasingly economic espionage.

John Carlin: This is a serious threat to our national security. I mean, our economy depends on the ability to innovate. And if there's a dedicated nation state who's using its intelligence apparatus to steal day in and day out what we're trying to develop, that poses a serious threat to our country.

Lesley Stahl: What is their ultimate goal, the Chinese government's ultimate goal?

John Carlin: They want to develop certain segments of industry and instead of trying to out-innovate, out-research, out-develop, they're choosing to do it through theft.

All you have to do, he says, is look at the economic plans published periodically by the Chinese Politburo. They are, according to this recent report by the technology research firm INVNT/IP, in effect, blueprints of what industries and what companies will be targeted for theft.

John Carlin: We see them put out the strategic plan, and then we see actions follow that plan. We see intrusion after intrusion on U.S. companies.

Lesley Stahl: Do you have a number of U.S. companies that have been hit?

John Carlin: It's thousands of actually companies have been hit.

Lesley Stahl: Thousands of U.S. companies?

John Carlin: Of U.S. companies.

### 2NC – Impact – Taiwan

#### Military modernization fuels aggression against Taiwan

Minnick 15 – (Wendell Minnick, B.S., M.A., is an author, commentator, journalist and speaker who has spent two decades covering military and security issues in Asia, including one book on intelligence and over 1,000 articles; 5/27/15, “White Paper Outlines China's Ambitions,” *Defense News*, <http://www.defensenews.com/story/defense/policy-budget/warfare/2015/05/26/china-us-pentagon-taiwan-report-south-east-sea-islands-reefs-s400-su35-missiles-satellite-space-deterrence/27957131/>, Accessed 6/29/16, HWilson)

The Chinese government report does make it clear that the military is implementing strategic guidelines of "active defense" in new maritime scenarios.

"In line with the evolving form of war and national security situation, the basic point for PMS [preparation for military struggle] will be placed on winning informationized local wars, highlighting maritime military struggle and maritime PMS."

The Chinese report states that the maritime environment is now a critical security domain. "The traditional mentality that land outweighs sea must be abandoned," it says. China will develop a "modern maritime military force structure commensurate with its national security and development interests, safeguard its national sovereignty and maritime rights and interests, protect the security of strategic SLOCs [sea lines of communication] and overseas interests, and participate in international maritime cooperation, so as to provide strategic support for building itself into a maritime power."

Taiwan appears doomed in both the Pentagon and Chinese report.

The Chinese report states that " 'Taiwan independence' separatist forces and their activities are still the biggest threat to the peaceful development of cross-Straits relations … the root cause of instability has not yet been removed."

The Pentagon report indicates that the primary driver of Chinese military modernization is a conflict over Taiwan. The self-ruled democratic island has resisted China's threats since the end of the Chinese civil war in 1949. The report indicates that Taiwan's multiple military variables to deter Chinese aggression are eroding. In the past, these have included China's inability to project sufficient power across the Taiwan Strait, the Taiwan military's technological superiority and the inherent geographic rewards of island defense.

#### China-Taiwan war draws in the US and goes nuclear

White 15 – (Hugh White AO is Professor of Strategic Studies at the Australian National University. His work focuses primarily on Australian strategic and defence policy, Asia-Pacific security issues, and global strategic affairs especially as they influence Australia and the Asia-Pacific; 5/5/15, “Would America Risk a Nuclear War with China over Taiwan?,” *The National Interest*, <http://nationalinterest.org/blog/the-buzz/would-america-risk-nuclear-war-china-over-taiwan-12808?page=show>, Accessed 6/29/16, HWilson)

After a decade of relative harmony, tensions between Beijing and Taipei are rising again. As Taiwan's leaders and voters face big choices about their future relations with China, America must think carefully about its commitments to Taiwan.

Would America be willing go to war with China to prevent Taiwan being forcibly united with the mainland? J. Michael Cole, responding in The National Interest to a recent op-ed of mine in Singapore's Straits Times, expresses a widely held assumption that it would, and should.

To many people it seems self-evident that America would honor the commitments enshrined in the Taiwan Relations Act. But the TRA was passed in 1979, when China's GDP was 1/20th the size of America's, its place in the global economy was miniscule, its navy and air force were negligible, and its prospects for progress depended completely on America's goodwill.

So back then a US-China conflict carried much bigger economic and military risks for China than for America. That made the TRA's commitments both highly credible and very unlikely to be tested. Washington could safely assume that Beijing would back off to avoid a conflict in which China had so much more to lose than America.

Things are different today.

China's economy is now so big and so central to global trade and capital flows that the consequences of any disruption would be just as serious for America as for China. Militarily, America can no longer expect a swift and certain victory in a war over Taiwan. China's anti-access/area-denial capabilities would preclude direct US intervention unless those capabilities had first been degraded by a sustained and wide-ranging strike campaign against Chinese bases and forces.

China would very likely respond to such a campaign with attacks on US and allied bases throughout Asia. The US has no evident means to cap the resulting escalation spiral, and no one could be sure it would stop below the nuclear threshold. The possibility of nuclear attacks on US cities would have to be considered.

These new realities of power mean that today a US-China conflict would impose equal risks and costs on both sides. And where costs and risks are equal, the advantage lies with those who have more at stake, and hence greater resolve. China's leaders today seem to think they hold this advantage, and they are probably right. It is therefore a big mistake to keep assuming, as many people seem to do, that China would be sure to back off before a crisis over Taiwan became a conflict.

### 2NC – Uniqueness – Espionage High

#### \*\*\*note when prepping file --- this answers the “Status Quo Solves” argument that Espionage is declining now

#### Chinese state-sponsored economic espionage is growing – FBI reports, corporate surveys, and past attempts prove

Bruer 15 – (Wes Bruer is a producer and writer covering Criminal Justice and National Security,7/24/15, “FBI sees Chinese involvement amid sharp rise in economic espionage cases,” *CNN Politics*, <http://www.cnn.com/2015/07/24/politics/fbi-economic-espionage/>, Accessed 6/29/16, HWilson)

The FBI has seen a sharp rise in economic espionage cases aimed at U.S. companies, with a vast majority of the perpetrators originating from China with ties to the nation's government, authorities said Thursday.

At a briefing at the FBI's Washington headquarters, the head of the agency's counterintelligence division, Randall Coleman, said the bureau has seen a 53% increase in economic espionage cases, or the theft of trade secrets leading to the loss of hundreds of billions of dollars, over the past year. He cited examples of large corporations successfully targeted in the past such as DuPont, Lockheed Martin and Valspar, who have since worked with the bureau to further safeguard their intellectual property.

To highlight this growing threat to the U.S. economy, the FBI has launched a nationwide campaign intended to warn industry leaders of the danger they face from foreign actors. But the FBI not only considers this a threat to American economic prosperity, but to its physical security as well.

"Economic security is national security," said Bill Evanina, the head of the National Counterintelligence and Security Center and one of the agents leading the charge in stemming the threat to corporations. Many of the tools used are the same as the ones used to track terrorists, he said.

In a survey conducted by the FBI, half of the 165 private companies that participated have claimed to be victims of economic espionage or theft of trade secrets, and 95% of those attempts originated from individuals associated with the Chinese government.

One of the most concerning means of obtaining sensitive industry secrets is through the use of "insider threats," or employees who are familiar with the inner workings of a particular technology being recruited by foreign agents in exchange for large amounts of cash.

"My company had first-hand experience dealing with an economic espionage case," Andy Ubel, the chief intellectual property counsel of Valspar, said in an FBI-produced video entitled "The Company Man: Protecting America's Secrets," which aims to "raise awareness of the growing economic espionage threat," the bureau says on its YouTube page.

"One of our key employees, a lab director, quit one day, and wouldn't tell us where he was going. And we only discovered later that he had downloaded a whole bunch of our data onto his own personal hard drive," Ubel said.

The FBI continues to see spear phishing attempts, when an email or link appears legitimate but is in fact a bogus message intended on tricking recipients into offering up personal information. Social media and sites like LinkedIn are also being utilized in economic espionage where potential recruits can be found and contacted based on relevant knowledge and work experience.

There have also been recent cases of trade secret theft which included dumpster diving for intellectual property such as discarded prototypes. In one case, the FBI says Chinese nationals were caught digging in corn fields in Iowa in search of seeds developed by a U.S. company to be pest and drought resistant. While the theft of corn seeds may appear innocuous, in reality the company that developed them spent tens of millions of dollars on research to perfect the technology.

"The Chinese government plays a significant role" in economic espionage, Evanina said. "The playing field is not level" when a single company faced with relentless targeting by individuals or entities who have the backing of a foreign government, he said.

### 2NC – Uniqueness – China Pursuing Semiconductors

#### China’s aggressively pursuing semiconductors right now through mergers and acquisitions – they’re convinced it’s key to national security – CFIUS review is key to their protection

Chu 16 – (Dr Ming-chin Monique Chu is Lecturer in Chinese Politics, Employability Officer within Social Sciences: Politics & International Relations at the University of Southampton, gained MPhil and PhD degrees in international relations from the University of Cambridge; 3/23/16, “China’s Ambitions in the Semiconductor Sphere and Taiwan’s Dilemma,” <https://sotonpolitics.org/2016/05/23/chinas-ambitions-in-the-semiconductor-sphere-and-taiwans-dilemma/>, Accessed 6/29/16, HWilson)\*\*\*note – the URL cited above is from a translation of this article originally published in Chinese at BBC News: <http://www.bbc.com/zhongwen/trad/china/2016/05/160506_china_semicounductor_business#orb-footer>

In recent years the Chinese government has systemically strived to improve the competitiveness of domestic semiconductor industry because of the national security importance of this industry. According to Chinese policy makers, a strong domestic semiconductor industry will become the cornerstone of the country’s economic development as well as its national defence.

As a result, Beijing has introduced various policies designed to increase local civilian firms’ competitiveness, market share, and research and development (R&D) capabilities. Efforts have also been made to increase the domestic supply of semiconductor chips, which have been largely imported so far.

Since 2001, Beijing has initiated a series of policies to help spur the spin-on in the Chinese context because of the dual-use nature of semiconductor technology and its recognition of the dominant spin-on trend in the global semiconductor industry. (The spin-on trend means that semiconductor technologies have predominantly flowed from the civilian side to the military because the former has become more superior to the latter in technological advancement.) Once China manages to improve its civilian firms’ semiconductor capabilities, the Chinese military can benefit from the technological transfers from the civilian side of the economy in its attempt to build a capable digitalized modern force, with improved precision strike capabilities and integrated abilities to operate in the battlefield.

It is little wonder that China has recently beefed up its efforts to engage in ambitious merger and acquisition (M&A) activities in the global semiconductor space in order to gain access to pertinent intellectual property (IP) in the pursuit of ascendancy in the strategic industry.

Some of the firms headquartered in the USA or Taiwan, two of the major players in the worldwide semiconductor sphere, have become the main targets. For instance, the Chinese state-owned Tsinghua Unigroup has attempted to acquire U.S. memory chip maker Micron Technology; it has also attempted to invest in U.S. hard-disk drive maker Western Digital, Taiwan’s integrated circuit (IC) design leader MediaTek, and three Taiwanese chip packaging companies. These three Taiwanese packaging firms include Silicon Precision Industries, ChipMOS Technologies, and Powertech Technology that together have more than 17% share of the global chip packaging capacity.

However, the U.S. regulators blocked the Chinese firm’s $23 billion offer to acquire Micron Technology on national security grounds last summer. In March the firm dropped its bid to become the biggest shareholder of Western Digital after the U.S. regulators had planned to investigate the deal.

### 2NC – AT: Non-Unique – Modernization Now

#### Even if there’s modernization now, China’s still behind the US, but Chinese espionage allows them to reverse that – prefer experts and recency

Wong 16 – (Kristina Wong, Pentagon, defense, and national security reporter at The Hill; citing Mark Gunzinger, senior fellow at the Center for Strategic and Budgetary Assessments, Chris Harmer, senior naval analyst at the Institute for the Study of War, Deputy Defense Secretary Bob Work and British Defense Procurement Minister Philip Dunne; 4/30/16, “Experts warn weapons gap is shrinking between US, Russia and China,” *The Hill*, <http://thehill.com/policy/defense/278262-experts-warn-weapons-gap-is-shrinking-between-us-and-competitors-russia-and>, Accessed 6/30/16, HWilson)

Competitors like Russia and China are closing the advanced weapons gap with the United States, aiming to push the U.S. out of areas on their front doorstep.

Experts say they're improving their ability to target U.S. aircraft and ships, pushing the U.S. military farther away from potential conflict zones and constraining its ability to use force in regions such as the Baltic Sea and the South China Sea.

"Since the end of the Cold War, the U.S. military has never really had to fight an enemy that had its own arsenal of precision-guided weapons," said Mark Gunzinger, senior fellow at the Center for Strategic and Budgetary Assessments.

"It was able to use air bases and other bases located fairly close to the borders of an enemy because there wasn't that much of an air and missile threat to those bases,” he said. “That’s changing.”

Experts say Russia and China are improving their ballistic and cruise missile technologies and hoping to create what they call “anti-access area-denial bubbles” where they can threaten U.S. air and ground operations.

Russia is in particular presenting a challenge to the U.S. in the Baltics region, where it has recently been harassing U.S. aircraft and ships.

”You’ve seen some advanced air-to-air technologies that the Chinese and Russians are developing, not just in stealth technology, but in terms of the advanced aerodynamics, advanced air-to-air radars, advanced air-to-air weapons, advanced air-to-ground weapons," said Chris Harmer, senior naval analyst at the Institute for the Study of War.

Experts say Russia and China are also making inroads into the U.S.’ undersea dominance.

"Chinese nuclear attack submarines are just in absolute overdrive, how quick they're building and how fast the technology is developing,” Harmer said. "And we've seen a significant increase in Russian naval activity, Russian long-range naval activity, Russian ships conducting port calls to Bandar Abbas in Iran.”

Iran, too, is making progress, experts say.

“They still lack a precision in their offensive weapons, and they're still trying to obtain and develop more effective air missile defenses, but they're making progress and their weapons are getting more accurate and their capabilities are increasing in their range, as well as in their numbers,” Harmer said. “The Iranian navy is getting a lot bigger a lot quicker than anybody expected.”

To keep ahead of those advances, the Pentagon is focusing on developing high-end weapons systems that can avoid detection even in close quarters, like the B-21 long-range stealth bomber.

It is also seeking to develop the high-end capabilities of allies like the United Kingdom in order to extend its reach.

Deputy Defense Secretary Bob Work and British Defense Procurement Minister Philip Dunne earlier this month toured U.S. military bases where the two nations are working closely together on advanced weapons systems.

That includes the F-35 Joint Strike Fighter, a fifth-generation stealth fighter; the P-8 Poseidon, a maritime patrol aircraft designed to detect foreign submarines and ships; and the Trident Class II D5 missile, which deploy from U.S. and Royal Navy ballistic missile submarines.

"I wouldn't say that these are specific towards any countries, but they're against high-end capabilities," Work said. "Countries like Iran are buying the most advanced air defense systems in the world … Advanced air defense systems are proliferating around the world. Submarine technology is proliferating around the world. They're becoming quieter, hard to find."

Work said the U.S. and the U.K.’s 25-year defense plan released last year would allow the two nations to be "interoperable in these high-end fights."

"If we ever projected power around the globe and the U.K. government said, 'We're with you,' we'd be interoperable from the top to the bottom," he said.

Some experts say the U.S. is not spending enough on weapons research and development.

"At the same time, the Russians and the Chinese — the Chinese more so than the Russians — are spending an awful lot of money on research and development,” Harmer said.

And cyber theft, particularly by the Chinese, is a problem, they add.

“Today, we're capable of losing in 10 seconds via cybercrime 10 years worth of research and development,” Harmer said. "And especially for the Chinese that's been a big help to them in closing the gap.”

#### Maybe there’s modernization now, but China’s not a challenger to the U.S. yet

Axe 15 – (David Axe is an American military correspondent who writes on military life and aspects of current conflicts, 6/22/15, “Why China is far from ready to meet the U.S. on a global battlefront,” *Reuters*, <http://blogs.reuters.com/great-debate/2015/06/21/why-china-is-far-from-ready-to-meet-the-u-s-on-a-global-battlefront/>, Accessed 6/30/16, HWilson)

Both of these statements are true:

1) China possesses a rapidly improving military that, in certain local or regional engagements, could match — and even defeat — U.S. forces in battle.

2) In military terms, China is a paper dragon that, despite its apparent strength, is powerless to intervene in world events far from its shores.

Seeing the distinction between these two ideas is the key to understanding China’s strategic aims, its military means and the threat, if any, that the country poses to its neighbors, the United States and the existing world order.

Beijing’s goals include “securing China’s status as a great power and, ultimately, reacquiring regional preeminence,” according to the 2015 edition of the U.S. Defense Department’s annual report on Chinese military power.

China is not a global military power. In fact, right now it doesn’t even want to be one.

But that doesn’t mean the world’s most populous country doesn’t pose a threat to the planet’s wealthiest and most powerful one. Yes, the United States and China are at odds, mostly as a result of China’s expanding definition of what comprises its territory in the western Pacific, and how that expansion threatens U.S. allies and the postwar economic order Washington was instrumental in creating.

### 2NC – AT: Military Superiority Inevitable

#### \*\*\*note when prepping file --- the Wong evidence below is also in the “2NC – AT: Non-Unique – Modernization Now” block above

#### They’re right that China is still behind the US, but Chinese espionage allows them to reverse that – prefer experts and recency

Wong 16 – (Kristina Wong, Pentagon, defense, and national security reporter at The Hill; citing Mark Gunzinger, senior fellow at the Center for Strategic and Budgetary Assessments, Chris Harmer, senior naval analyst at the Institute for the Study of War, Deputy Defense Secretary Bob Work and British Defense Procurement Minister Philip Dunne; 4/30/16, “Experts warn weapons gap is shrinking between US, Russia and China,” *The Hill*, <http://thehill.com/policy/defense/278262-experts-warn-weapons-gap-is-shrinking-between-us-and-competitors-russia-and>, Accessed 6/30/16, HWilson)

Competitors like Russia and China are closing the advanced weapons gap with the United States, aiming to push the U.S. out of areas on their front doorstep.

Experts say they're improving their ability to target U.S. aircraft and ships, pushing the U.S. military farther away from potential conflict zones and constraining its ability to use force in regions such as the Baltic Sea and the South China Sea.

"Since the end of the Cold War, the U.S. military has never really had to fight an enemy that had its own arsenal of precision-guided weapons," said Mark Gunzinger, senior fellow at the Center for Strategic and Budgetary Assessments.

"It was able to use air bases and other bases located fairly close to the borders of an enemy because there wasn't that much of an air and missile threat to those bases,” he said. “That’s changing.”

Experts say Russia and China are improving their ballistic and cruise missile technologies and hoping to create what they call “anti-access area-denial bubbles” where they can threaten U.S. air and ground operations.

Russia is in particular presenting a challenge to the U.S. in the Baltics region, where it has recently been harassing U.S. aircraft and ships.

”You’ve seen some advanced air-to-air technologies that the Chinese and Russians are developing, not just in stealth technology, but in terms of the advanced aerodynamics, advanced air-to-air radars, advanced air-to-air weapons, advanced air-to-ground weapons," said Chris Harmer, senior naval analyst at the Institute for the Study of War.

Experts say Russia and China are also making inroads into the U.S.’ undersea dominance.

"Chinese nuclear attack submarines are just in absolute overdrive, how quick they're building and how fast the technology is developing,” Harmer said. "And we've seen a significant increase in Russian naval activity, Russian long-range naval activity, Russian ships conducting port calls to Bandar Abbas in Iran.”

Iran, too, is making progress, experts say.

“They still lack a precision in their offensive weapons, and they're still trying to obtain and develop more effective air missile defenses, but they're making progress and their weapons are getting more accurate and their capabilities are increasing in their range, as well as in their numbers,” Harmer said. “The Iranian navy is getting a lot bigger a lot quicker than anybody expected.”

To keep ahead of those advances, the Pentagon is focusing on developing high-end weapons systems that can avoid detection even in close quarters, like the B-21 long-range stealth bomber.

It is also seeking to develop the high-end capabilities of allies like the United Kingdom in order to extend its reach.

Deputy Defense Secretary Bob Work and British Defense Procurement Minister Philip Dunne earlier this month toured U.S. military bases where the two nations are working closely together on advanced weapons systems.

That includes the F-35 Joint Strike Fighter, a fifth-generation stealth fighter; the P-8 Poseidon, a maritime patrol aircraft designed to detect foreign submarines and ships; and the Trident Class II D5 missile, which deploy from U.S. and Royal Navy ballistic missile submarines.

"I wouldn't say that these are specific towards any countries, but they're against high-end capabilities," Work said. "Countries like Iran are buying the most advanced air defense systems in the world … Advanced air defense systems are proliferating around the world. Submarine technology is proliferating around the world. They're becoming quieter, hard to find."

Work said the U.S. and the U.K.’s 25-year defense plan released last year would allow the two nations to be "interoperable in these high-end fights."

"If we ever projected power around the globe and the U.K. government said, 'We're with you,' we'd be interoperable from the top to the bottom," he said.

Some experts say the U.S. is not spending enough on weapons research and development.

"At the same time, the Russians and the Chinese — the Chinese more so than the Russians — are spending an awful lot of money on research and development,” Harmer said.

And cyber theft, particularly by the Chinese, is a problem, they add.

“Today, we're capable of losing in 10 seconds via cybercrime 10 years worth of research and development,” Harmer said. "And especially for the Chinese that's been a big help to them in closing the gap.”

#### The U.S. may spend more, but China’s strategically investing in specific capabilities that’s making them a real threat in the near future

Heinrichs 14 – (Rebeccah L. Heinrichs is a fellow at the George C. Marshall Institute where she writes about defense and foreign policy and specializes in nuclear deterrence and missile defense; 10/24/14, “China patiently challenges US military superiority,” *The Hill*, <http://thehill.com/blogs/congress-blog/foreign-policy/221665-china-patiently-challenges-us-military-superiority>, Accessed 6/30/16, HWilson)

While the U.S. reacts to the scourges of Ebola and ISIS, China continues to patiently and steadily exploit weaknesses in U.S. military capabilities. The bipartisan U.S. China Commission is poised to release its annual report to Congress that details some of the specifics. The big lesson to learn from it is that the U.S. can not only react to world events, it must also look forward and prepare to deter and defend against distant and not-so-distant threats. For as hard as it is to beat back ISIS, a terror organization with a lot of motivation but without serious military might, imagine the fix in which the U.S. will find itself with a China whose national objectives conflict with the U.S., and with the military capabilities to see them out.

According to the Washington Free Beacon’s Bill Gertz who obtained the report, the PLA has deployed two brigades of DF-21D ballistic missiles, infamously called “carrier killers.” In December of 2010, then Commander of the U.S. Pacific Command, Admiral Willard, revealed China was developing these lethal missiles but emphasized that they had merely achieved what the U.S. called “initial operational capability” meaning, the PLA was still developing the system and that it had not fully matured.

Four years later, the missiles have presumably been improved and have multiplied. China has opted not to flight test the missile, keeping the U.S. guessing on whether or not its primary military platform for deterring war and keeping peace in the region—the aircraft carrier—can be directly targeted. The U.S. has no defensive system in its arsenal that could defeat the highly sophisticated DF-21D. But this isn’t the only Achilles Heal the Chinese have been working to expose.

Indeed, this has been China’s objective: rather than trying to compete with the U.S by building a conventional military that goes toe to toe with the Pentagon’s, and thereby draining its resources, it is developing high-technology weapons that directly challenge where the U.S. is weakest. This is why it’s a bad argument to insist that since the U.S. defense budget dwarfs the Chinese defense budget, it necessarily means the U.S. can dismiss the Chinese (or Russian, or North Korean or Iranian, for that matter) threats.

Of particular concern is China’s emphasis on nuclear capabilities, which the Obama administration has opted not to detail in its annual reports to Congress. According to Gertz, “The commission report faults the Pentagon for ending its practice of providing details of China’s nuclear arsenal in annual reports to Congress, saying the omission is contributing to Chinese military secrecy.” And actually, the Obama Pentagon stopped releasing its annual report on China’s missile force after its 2010 report. The complete absence of these reports, combined with the administration’s patterns of conciliatory outreach towards Beijing, make it seem like the Obama administration doesn’t want to put public pressure on the Chinese government for its aggressive military developments designed to threaten the U.S.

But Frank Kendall, the Under Secretary of Defense for Acquisition, Technology and Logistics has recently been sounding an alarm bell, urging industry to bring him new ideas, to innovate, and to fight for the U.S. strategic edge.

In August he raised eyebrows by saying, “Our technological superiority is very much at risk, there are people designing systems [specifically] to defeat us in a very thoughtful and strategic way, and we’ve got to wake up, frankly.” Just this month he provided a document to Congressional staff laying out key warfare domains where the U.S. is losing superiority. To name a few of those key domains listed in the document: China could target the U.S. surface fleet and overseas bases at risk in the Western Pacific; could challenge U.S. dominance of the air by the year 2020; is rapidly advancing in space and could prevent the functionality of U.S. satellites; and continues its cyber assault on U.S. computer networks.

As if aware of how startled the document could leave its readers, Kendall says in the summary section, “The intent of this paper is not to suggest that military confrontation with China is inevitable or likely.” Then he goes on to close with this: “Technological superiority the U.S. demonstrated over 20 years ago, and which we have relied upon ever since, is being actively challenged.” U.S. policy-makers and especially the next administration better read between the lines. It is because of the latter quote that makes confrontation all the more likely.

#### \*\*\*note when prepping file --- the warrants in the evidence below are all in the previous card, so reading this card would just be repetitive, but I’m including it

#### ---more evidence

AFP 14 – (Agence France-Presse is an international news agency headquartered in Paris, France. Founded in 1944, AFP is the third largest news agency in the world, after the Associated Press and Reuters; cites Frank Kendall, the Pentagon's chief weapons buyer and Admiral Samuel Locklear, head of US Pacific Command; 1/29/14, “China Is Challenging US Military Superiority, Says Pentagon Official,” *Business Insider*, <http://www.businessinsider.com/china-is-challenging-us-military-superiority-2014-1>, Accessed 6/30/16, HWilson)

China poses an increasing challenge to the US military's technological edge while budget pressures are hampering Washington's effort to stay ahead, a senior defense official warned on Tuesday.

Frank Kendall, the Pentagon's chief weapons buyer, told lawmakers that when it comes to "technological superiority, the Department of Defense is being challenged in ways that I have not seen for decades, particularly in the Asia-Pacific region."

Citing China's major investments in anti-ship missiles, stealth fighter jets, hypersonic vehicles and other hi-tech weaponry, Kendall said the United States could lose its dominant position if it failed to respond to the altered strategic landscape.

"Technological superiority is not assured and we cannot be complacent about our posture," he told the House Armed Services Committee.

Asked to assess what one lawmaker called an arms race between the two countries, Kendall said there was cause for concern as China dramatically increases its military spending.

"Their budget is far smaller than ours, but their personnel costs are also far smaller than ours," said Kendall, undersecretary of defense for acquisition, technology and logistics.

"Our budgets are going in the opposite direction. So just by that metric alone, it's not positive."

Lawmakers and defense analysts say China is making strides in modernizing its military, particularly in the area of so-called "anti-access" weapons -- such as missiles and electronic jamming systems -- that could potentially limit the reach of US aircraft carriers or warplanes.

Kendall said when he returned to the Pentagon after being away for 15 years, he was "struck immediately by the nature, scope and quality of the investments that are being made in A2AD, as we call it, anti-access area denial capabilities."

As a result, the Pentagon is "looking very carefully at Pacific Command's requirements and what they need for the operations in that area," he said.

Kendall added that Washington was concerned about China exporting its newer weapons abroad.

Echoing Kendall's wider concerns, Admiral Samuel Locklear, head of US Pacific Command, said last week that the American military's "relative dominance" is declining as other countries invest in sophisticated weapons.

### 2NC – Internal Link – Mergers/Acquisitions Key / AT: CFIUS Not Key

#### \*\*\*note when prepping file --- this card is also under the header “2NC – Uniqueness – China Pursuing Semiconductors” above

#### China’s aggressively pursuing semiconductors right now, specifically through through mergers and acquisitions – they’re convinced it’s key to national security – CFIUS review is key to their protection

Chu 16 – (Dr Ming-chin Monique Chu is Lecturer in Chinese Politics, Employability Officer within Social Sciences: Politics & International Relations at the University of Southampton, gained MPhil and PhD degrees in international relations from the University of Cambridge; 3/23/16, “China’s Ambitions in the Semiconductor Sphere and Taiwan’s Dilemma,” <https://sotonpolitics.org/2016/05/23/chinas-ambitions-in-the-semiconductor-sphere-and-taiwans-dilemma/>, Accessed 6/29/16, HWilson)\*\*\*note – the URL cited above is from a translation of this article originally published in Chinese at BBC News: <http://www.bbc.com/zhongwen/trad/china/2016/05/160506_china_semicounductor_business#orb-footer>

In recent years the Chinese government has systemically strived to improve the competitiveness of domestic semiconductor industry because of the national security importance of this industry. According to Chinese policy makers, a strong domestic semiconductor industry will become the cornerstone of the country’s economic development as well as its national defence.

As a result, Beijing has introduced various policies designed to increase local civilian firms’ competitiveness, market share, and research and development (R&D) capabilities. Efforts have also been made to increase the domestic supply of semiconductor chips, which have been largely imported so far.

Since 2001, Beijing has initiated a series of policies to help spur the spin-on in the Chinese context because of the dual-use nature of semiconductor technology and its recognition of the dominant spin-on trend in the global semiconductor industry. (The spin-on trend means that semiconductor technologies have predominantly flowed from the civilian side to the military because the former has become more superior to the latter in technological advancement.) Once China manages to improve its civilian firms’ semiconductor capabilities, the Chinese military can benefit from the technological transfers from the civilian side of the economy in its attempt to build a capable digitalized modern force, with improved precision strike capabilities and integrated abilities to operate in the battlefield.

It is little wonder that China has recently beefed up its efforts to engage in ambitious merger and acquisition (M&A) activities in the global semiconductor space in order to gain access to pertinent intellectual property (IP) in the pursuit of ascendancy in the strategic industry.

Some of the firms headquartered in the USA or Taiwan, two of the major players in the worldwide semiconductor sphere, have become the main targets. For instance, the Chinese state-owned Tsinghua Unigroup has attempted to acquire U.S. memory chip maker Micron Technology; it has also attempted to invest in U.S. hard-disk drive maker Western Digital, Taiwan’s integrated circuit (IC) design leader MediaTek, and three Taiwanese chip packaging companies. These three Taiwanese packaging firms include Silicon Precision Industries, ChipMOS Technologies, and Powertech Technology that together have more than 17% share of the global chip packaging capacity.

However, the U.S. regulators blocked the Chinese firm’s $23 billion offer to acquire Micron Technology on national security grounds last summer. In March the firm dropped its bid to become the biggest shareholder of Western Digital after the U.S. regulators had planned to investigate the deal.

#### A litany of past hacks prove that hacks are conducted through government sponsored corporate entities

Dennis 15 – (Neal Dennis recently joined ASERT as a Threat Intelligence Analyst. For more than 13 years during his time prior to Arbor, he supported various military cyber elements, including USCYBERCOM and 24th Air Force. He has worked in most levels of cyber operations, from network defense and sitting on the wire to strategic intelligence support; 8/17/15, “Espionage, Spying and Big Corporate Data, These Are a Few of China’s Favorite Things,” <https://www.arbornetworks.com/blog/asert/espionage-spying-and-big-corporate-data-these-are-a-few-of-chinas-favorite-things/>, Accessed 7/1/16, HWilson)

For those keeping score, the United States Office of Personnel Management (OPM), Anthem, Premera, and Carefirst Blue Cross all reported large data breaches, seemingly perpetrated by the same possible Chinese state-sponsored threat actors [1]. Research into the OPM breach provided information leading investigators to believe the same group of threat actors also compromised additional companies [2]. These investigators released IOC’s that United Airlines used to detect their own data breach in late May/early June of 2015. The data stolen reportedly included passenger manifests containing travel information and basic demographics about travelers. Additionally, according to Bloomberg, one of the individuals familiar with the case indicated information regarding United’s corporate merger and acquisition strategy was also possibly compromised.

Considering the context discussed so far, let’s highlight the current train of thought amongst many in the security industry. Most people believe this information is likely being used by China’s intelligence apparatus to develop a sort of “Facebook” repository of U.S. government personnel possibly to be used in ongoing and future intelligence gathering operations. Indeed, all the medical data and OPM information would be of great use to any nation desiring to gather intelligence or support operations against the United States. Individuals have gone on to suggest the United Airlines breach may have supported human intelligence (HUMINT) collection operations, since it would have potentially allowed threat actors to track traveler movement.

The Flip

While this popular intelligence angle certainly represents a valid assessment, what if the United Airlines breach, and possibly the healthcare breaches, were motivated by an alternative objective? In May of 2014, a U.S. grand jury indicted five Chinese military hackers (the APT1 group) on 31 counts of corporate cyber espionage related charges [3]. According to the U.S. Federal government, China is known to use government assets to support their commercial and economic endeavors.

### 2NC – Link – CFIUS

#### \*\*\*note when prepping file --- this also answers the “Status Quo Solves” argument that espionage is declining now because some of these cards make the claim that espionage is coming now

#### Chinese SOEs are a likely inroad for Chinese espionage – maintaining unfettered CFIUS review is key

Stanley 15 – (Mary Ellen Stanley, B.A., University of Richmond (2011); M.A., Baylor University (2013); J.D., Brooklyn Law School (Expected 2016); Editor-in-Chief, Brooklyn Journal of International Law (2015-2016); Fellow, Dennis J. Block Center for the Study of International Business Law (2014-2016); 2015, “From China with Love: Espionage in the Age of Foreign Investment,” Published in *Brooklyn Journal of International Law*, Vol.40, Issue 3, pgs 1033-1079; <http://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1113&context=bjil>, Accessed 6/24/16, HWilson)

Throughout U.S. history, national security has been a paramount concern of the U.S. government. 15 In recent decades, burgeoning technologies and the rise of unconventional acts of terror have heightened fears for the nation’s security. These fears have resulted in the perception of new threats to the nation’s security and a labyrinthine definition of “national security.”16 Conventional acts of espionage––those primarily associated with identifiable persons or groups––have conceptually merged with cybersecurity breaches and industrial espionage.17 The Federal Bureau of Investigation (“FBI”) notably remarked that “[t]he Cold War is not over, it has merely moved to a new arena: the global marketplace.”18 This amalgamation of threats has created a “poisoned climate” in which to balance the nation’s economic prosperity and national security.19 In this environment, cyber-espionage has threatened prominent U.S. businesses, including Home Depot and J.P. Morgan Chase.20 These events illustrate widespread flaws in corporate and government security across the globe.

As globalization accelerates and the world’s largest corporations conduct cross-border transactions with increasing frequency,21 businesses can be victims of espionage, or instead become vessels for espionage through FDI.22 This can occur in two ways: first, when a State-owned or government-connected entity conducts business in the United States; and second, when a foreign entity purchases a U.S. business.23 Foreign ownership of U.S. entities establishes a foreign presence in the United States and enables theft of “American technology, intellectual property, and sensitive information pertaining to critical infrastructure.” 24

While the FBI, Central Intelligence Agency, and National Security Agency address certain security concerns stemming from foreign investments, CFIUS is the government agency charged with preserving this nuanced component of national security.25 CFIUS is an inter-agency committee of the U.S. government26 and is authorized to review transactions that could “result in control of a U.S. business by a foreign person.” 27 CFIUS conducts such reviews to determine whether certain transactions pose national security threats.28 However, this review places an additional burden on CFIUS’s duties as a governmental agency. CFIUS must maintain and protect U.S. national security while simultaneously balancing the business interests of foreign investors.29

#### CFIUS monitoring is key to protect against espionage-related acquisitions

Baker and Heifetz 10 – (Stewart Baker, first Assistant Secretary for Policy at the Department of Homeland Security, and served in the Department of Justice and the Department of Homeland Security (DHS), as well as the Central Intelligence Agency. In his most recent government position, he served as Deputy Assistant Secretary and Acting Assistant Secretary for the Office of Policy Development at DHS; September 2010, “Addressing National Security Concerns,” Published in *Policy Insight*, <http://www.steptoe.com/assets/attachments/4149.pdf>, Accessed 6/27/16, HWilson)

The analytical inquiry assesses the threat, vulnerability and consequence of a foreign acquisition of an American target. Discussions generally focus on the acquirer’s intent and ability to cause harm (the threat), whether and how the target assets might be exploited to breach national security (the vulnerability) and the consequences of a successful exploitation of American resources (the consequence). These factors guide the Committee’s efforts to protect against espionage, illicit acquisitions of sensitive technology and the risk of mass casualties, among other concerns.

The Emcore-Tangshan deal likely raised concerns because of the role of Emcore’s fiber optics products in highly strategic and espionage-vulnerable U.S. communications systems. This deal is the third Chinese investment in less than three years that has been abandoned publicly because of CFIUS. Some of the concerns the CFIUS review raised can be attributed to widespread publicity over alleged Chinese hacking of U.S. networks, raising deep suspicions about espionage.

Congressional concerns

When the Congressional Steel Caucus urged CFIUS to examine the deal between Steel Development Co. and Anshan Iron & Steel Group in July, the U.S. lawmakers expressed concerns about the effect of Chinese investment on U.S. steel markets and Chinese access to American steel production technologies.

#### CFIUS review is crucial to determine which acquisitions actually pose a threat – most qualled

Graham 06 – (Edward M. Graham (1944–2007) was a senior fellow at the Peterson Institute from 1990 to 2007. He also taught concurrently as adjunct professor at Columbia University in New York. Previously he was an economist at the US Treasury and taught full-time in the business schools of several US universities (MIT, University of North Carolina Chapel Hill, Duke University, among others). While serving at the Treasury, he was seconded for two years to the Organization for Economic Cooperation and Development (OECD) in Paris. He also served as visiting or adjunct faculty at the University of Virginia, Charlottesville; Stanford University (Washington Program); The Johns Hopkins University; Seoul National University; Harvard University (John F. Kennedy School of Government); INSEAD (European Institute of Administration, Fontainebleau, France); and the University of Paris I (Pantheon/La Sorbonne). His research interests have included foreign direct investment, international competition policy, and the industrial organization of major Asian economies; 7/1/06, “How China Can Break Down America's Wall,” Published in the *Far Eastern Economic Review*, <https://piie.com/commentary/speeches-papers/how-china-can-break-down-americas-wall>, Accessed 6/27/16, HWilson)

Government ownership of companies often raises questions of whether they will make decisions based on commercial interests or national interest. Given America’s strategic concerns with Beijing, the fact that so many Chinese companies are controlled by the state will result in exacting scrutiny of Chinese investments under the US government process for reviewing the national security implications of foreign investments. This process, conducted by the 12-agency Committee on Foreign Investment in the United States (CFIUS), was created in 1988 at precisely the time when Congress was concerned about growing investments from Japan.

But government ownership is not the only factor likely lead to extra scrutiny by CFIUS. The possibility of sensitive, export-controlled technology being transferred to other countries is a factor in virtually all reviews by the committee, regardless of the home country of the acquirer. It is a concern in the case of Chinese acquisitions largely because of a series of high-profile breaches of US export-control laws and regulations by Chinese companies in the late 1990s and early 2000s. China’s espionage activities have become a concern to US counterintelligence agencies, including the Department of Justice, Defense, and Homeland Security, as well as the Federal Bureau of Investigation. These agencies are worried that certain Chinese companies might be used as covers for intelligence operations. So long as the Pentagon views China suspiciously, CFIUS will likely assess Chinese acquisitions of US companies in part on their impact on China’s military strength.

Chinese acquisitions may also present different economic issues for US policy makers to consider. For example, whereas a significant number of Japanese investments flowed into the US manufacturing sector as greenfield investments, Chinese companies have many comparative advantages, including low labor costs, in manufacturing and already have significant access to the US market. Chinese companies may be less interested in establishing a manufacturing base in the United States than in developing globally competitive management skills and global brand names. Moreover, Chinese companies are keenly interested in acquisitions in strategic sectors, including energy—precisely those sectors that may raise political or national security issues in the United States.

#### CFIUS review is critical to prevent theft of military secrets

Graham and Marchick 06 – (Edward M. Graham (1944–2007) was a senior fellow at the Peterson Institute from 1990 to 2007. He also taught concurrently as adjunct professor at Columbia University in New York. Previously he was an economist at the US Treasury and taught full-time in the business schools of several US universities (MIT, University of North Carolina Chapel Hill, Duke University, among others). While serving at the Treasury, he was seconded for two years to the Organization for Economic Cooperation and Development (OECD) in Paris. He also served as visiting or adjunct faculty at the University of Virginia, Charlottesville; Stanford University (Washington Program); The Johns Hopkins University; Seoul National University; Harvard University (John F. Kennedy School of Government); INSEAD (European Institute of Administration, Fontainebleau, France); and the University of Paris I (Pantheon/La Sorbonne). His research interests have included foreign direct investment, international competition policy, and the industrial organization of major Asian economies; David M. Marchick serves as Managing Director and Global Head of External Affairs and serves as a Member of The Carlyle Group’s Management Committee, and formerly was partner and Vice-Chair of the international practice group at Covington & Burling. He is an expert on foreign investment and national security issues; May 2006, “US NATIONAL SECURITY AND FOREIGN DIRECT INVESTMENT,” Published by the Peterson Institute for International Economics, <https://piie.com/publications/chapters_preview/3918/04iie3918.pdf>, Accessed 7/1/16, pgs 112-115, HWilson)

Espionage

In recent years, China's espionage activities have become an increasing concern and a higher priority to the relevant US government agencies involved in counterintelligence activities, including the Department of Jus- tice (DOJ), the DOD, the Department of Homeland Security (DHS), and the FBI. The specter of significant, targeted Chinese espionage activities in the United States first hit public consciousness in the late 1990s with a widely publicized and controversial report by a select committee of the House of Representatives, chaired by Christopher Cox (R-CA)—the so- called Cox Report—and the allegations that Wen Ho Lee, a scientist working at Los Alamos National Laboratory in New Mexico, shared nuclear secrets with the Chinese.38 The espionage charges against Wen Ho Lee were ultimately dropped, although he did plead guilty to a lesser charge of mishandling classified information. The Cox Report found, among other things, that China had stolen design information on the United States' most advanced thermonuclear weapons, and that Chinese penetration of US national laboratories reached back several decades (US House of Representatives 1999, overview section ii). The report concluded that the United States did not have adequate safeguards against Chinese espionage at US national laboratories. China had mounted a "widespread effort to obtain US military technology by any means—legal or illegal" and US counterintelligence efforts had been "complicate[d]" because China conducted espionage activities in a "less centralized" manner than did the Soviet Union during the Cold War (US House of Representatives 1999).

Subsequent reports and articles suggest that Chinese espionage activities are receiving increased attention from the US counterintelligence community. In an August 10, 2005, front page Wall Street Journal report, entitled "FBI Sees Big Threat from Chinese Spies," David Szady, the FBI's top counterintelligence official, stated, "China is the biggest [espionage] threat to the US today." The FBI had "sent hundreds of new counterintelligence agents" throughout the United States, many with "a specific focus on China." Further, the perceived threat was much different from that posed previously by the Soviet Union. Unlike the Soviets, literally "thou- sands of Chinese nationals" come every year to the United States as "students and businessmen." These Chinese nationals, the story continued, are contacted by Chinese government officials, who press them into service to "acquire military or industrial technology illegally."39

The Wall Street Journal's coverage echoes public reports by the Central Intelligence Agency (CIA). In their 1999 Report to Congress on Chinese Espionage Activities Against the United States, the CIA and FBI conclude that "much of China's intelligence collection in 1998 continued to be accomplished by a network of nonprofessional individuals and organizations act- ing outside the direction and control of the intelligence services." Further, "some of the thousands of Chinese students, scientists, researchers, and other visitors to the United States also gather information, working mostly for the benefit of government-controlled, end-user organizations and other scientific bureaus, research institutions, and enterprises." Finally, "China's commercial entities play a significant role in the pursuit of proprietary US technology. According to the CIA, the vast majority of Chinese commercial entities in the United States are legitimate companies; however, some are a platform for intelligence collection activities" (US CIA and FBI 1999). It seems clear that US officials involved in counterintelligence activities view China as a real threat, and have identified Chinese companies, students, and researchers as a conduit for state-sponsored commercial and military espionage activities.

How does this affect a CFIUS analysis of a Chinese acquisition in the United States? We suspect that, at a minimum, the potential for espionage almost certainly will be a factor in many CFIUS reviews of acquisitions of US companies by Chinese entities. CFIUS agencies will also likely scrutinize a Chinese company's leadership and their ties, or alleged ties, to Chinese intelligence agencies and the military. If CFIUS agencies have concerns about the increased risk of espionage because of a transaction, they may block the transaction, or impose safeguards to mitigate the risk.

Strengthening the Chinese Military

The Pentagon's 2005 report to Congress on China's military power (Pentagon Report) states in unequivocal terms that the growth and strengthening of China's military threatens US interests (US DOD 2005). In the executive summary, it states, "If current trends [toward strengthening of China's military] persist, PLA [People's Liberation Army] capabilities could pose a credible threat to other modern militaries operating in the region." In addition to describing what it regards as worrying trends in China's force structure, strategies, and defense procurement budgets, the Pentagon Report makes clear that the DOD views the development of China's economy and technology base, and the strengthening of its military, as intertwined. It quotes Chinese President Hu Jintao as saying, "It is necessary to establish a mechanism of mutual promotion and coordinated development between national defense building and economic development," inferring from President Hu's statement that "China's modernization indicates a buildup of armaments that reinforces this notion of coordinated, integrated civilian and military development" (US DOD 2005, 11). The report also asserts that China is actively seeking dual-use and military technologies from the European Union, Israel, Russia, and other countries (US DOD 2005, 23) and that China seeks to "accelerate its military development by using more of its civil production capacity for military hardware" (US DOD 2005,13).

To illustrate how CFIUS might distinguish between acquisitions of the same US entity by companies based in three different countries, assume that either a Chinese or Pakistani entity were buying a small US company that owned sensitive, export-controlled technologies. If CFIUS was concerned that the technology or manufacturing within this company was critical to US defense capabilities, and that the technology would be transferred offshore, CFIUS would either reject the acquisition, or use a mitigation agreement to prohibit the transfer of technology or movement of manufacturing offshore. If CFIUS was concerned that there would be no way to control technology transfer, or have assurances that it would not happen, CFIUS would likely reject the acquisition by both the Chinese and Pakistani entities. However, if the sole concern of the sale was that its acquisition would strengthen the military capabilities of the acquirer, then the Chinese company might be turned down while the Pakistani company was allowed to proceed, since Pakistan's military is not seen as a threat to the United States.

As long as the Pentagon takes such a negative view of China, CFIUS will likely assess Chinese acquisitions of US companies in part on their impact on China's military strength. This approach turns the traditional CFIUS approach on its head. Rather than focusing on whether an acquisi- tion threatens to reduce the DOD's and other national security agencies' access to goods and services for US national defense, CFIUS instead will consider whether an acquisition strengthens the Chinese military's access to goods and services. Thus weakening the United States and strengthen- ing our enemies can be seen as two sides of the same national security coin.

CFIUS will therefore likely analyze not only the sophistication of dual- use technologies owned or developed by a target company, but also the ties of the Chinese acquirer to the Chinese military-industrial complex. Recent testimony by Evan Medeiros, an expert on China's military at the Rand Corporation, a think tank influential with the Pentagon, identifies 11 SOEs that "have historically always been involved in production of military goods."40 These SOEs are the China National Nuclear Group Corpo- ration (www.cnnc.com.cn), China Nuclear Engineering and Construction Group Corporation (www.cnecc.com.cn), China Aerospace Science and Technology Group Corporation (www.cascgroup.com.cn), China Aero- space Science and Industry Group Corporation (www.casic.com.cn), China Aviation Industry Group Corporation I (wmv.avicl.com.cn), China Avi- ation Industry Group Corporation II (www.avic2.com.cn), China State Shipbuilding Group Corporation (mvw.cssc.net.cn), China Shipbuilding Industry Corporation (www.csic.com.cn), China North Industries Group Corporation (www.norincogroup.com.cn), China South Industries Group Corporation (www.chinasouth.com.cn), and China Electronics Technol- ogy Group Corporation (wmv.cetc.com.cn).

If the Pentagon agrees with Medeiros's assessment, these 11 companies (and other companies on DOD's own list) could face additional challenges in clearing CFIUS, depending on the sensitivity of the target company in the United States.41 Any Chinese acquirer must accordingly account for and, if necessary, rebut perceptions about its relationship with the Chinese military to navigate the CFIUS process successfully.

### 2NC – AT: China-US Cyber Agreement Solves

#### It doesn’t solve – doesn’t contain binding rules and exceptions exist

Zetter 15 – (Kim Zetter is an award-winning, senior staff reporter at Wired covering cybercrime, privacy, and security; 9/25/16, “US and China Reach Historic Agreement on Economic Espionage,” *Wired*, <https://www.wired.com/2015/09/us-china-reach-historic-agreement-economic-espionage/>, Accessed 6/29/16, HWilson)

China, however, has long been suspected of spying on companies in the US defense, tech, and energy sectors in order to advance Chinese businesses and innovations. President Xi did not publicly acknowledge the activity but agreed with Obama at the press conference that “confrontation and friction are not the right choice for both sides.” He also reportedly agreed to become more cooperative in responding to US law enforcement requests in seeking aid to track down cybercriminals in China.

Obama said the US would be watching closely to determine whether “words are followed by actions” and would not hesitate to use sanctions and other “tools” against China for such activity.

China, of course, has been implicated in the recent massive hack against the Office of Personnel Management, which involved the theft of sensitive data on some 21 million people, including the fingerprint records of more than 5 million federal workers, many of whom hold security clearances and use their fingerprints to gain access to secured facilities.

This, however, is not the kind of hacking that would be barred under the new agreement, since it falls under traditional categories of nation-state spying. The agreement barring economic spying refers to other attacks, such as ones against Google and some 30 other tech companies in 2010 that aimed to steal their source code, as well as the kinds of breaches allegedly conducted by five Chinese hackers whom the US government indicted last year. All five, who are said to be associated with China’s People’s Liberation Army, are accused of stealing information from six companies in the energy, metals, and manufacturing industries.

The FBI said in a report released earlier this year that economic espionage cases in the US surged 53 percent in 2014, and that China was responsible for most of it.

Congressman Jim Langevin (D-Rhode Island), a senior member of the House Armed Services and Homeland Security Committees, expressed cautious optimism at the news.

“This agreement represents important, substantive progress in the relationship between the U.S. and China,” he said in a statement. “For too long, Chinese hackers—both governmental and criminal—have exploited American companies by stealing their hard-won intellectual property and using it to further their own economic interests. This accord clarifies that so-called ‘economic espionage’ is not espionage but theft and that it has no place in 21st century dealings between states.”

He noted, however, that he remains skeptical about the Chinese commitment to carry out the agreement.

“I believe that the threat of sanctions brought President Xi to the negotiating table, and President Obama must make clear to his counterparts that sanctions will be levied on rogue actors in cyberspace.”

#### It doesn’t solve – disagreements are still prevalent

Bloomberg 15 – (Bloomberg News Agency citing no author; 9/23/15, “U.S.-China hacking deal likely to skip industrial espionage for now,” <http://www.japantimes.co.jp/news/2015/09/23/asia-pacific/u-s-china-hacking-deal-likely-to-skip-industrial-espionage-for-now/#.V3IEHbgrJhG>, Accessed 6/28/16, HWilson)

HONG, KONG/ WASHINGTON/SEATTLE – Disputes over what is acceptable behavior in cyberspace threaten to overshadow the agenda when Chinese President Xi Jinping and U.S. President Barack Obama meet in Washington late this week.

The simmering conflict over hacking comes at a time when the U.S. is seeking cooperation with China on issues ranging from North Korea to anti-terrorism and climate change.

Xi will arrive in Washington on Thursday for a two-day visit.

Xi said Tuesday that China was ready to set up a mechanism with the U.S. to fight cybercrime. Speaking in Seattle on the first day of his weeklong U.S. visit, Xi told a gathering of business leaders that China is a staunch defender of cybersecurity and was prepared to establish a “high-level” forum with the U.S. to address mutual hacking concerns.

Addressing former U.S. Secretary of State Henry Kissinger, Microsoft Corp. co-founder Bill Gates and other guests at a banquet, Xi said “both commercial cybertheft and hacking against a government’s networks are crimes that must be punished in accordance with law of relevant international treaties.” He called on the international community to work together to build “a peaceful, secure and cooperative cyberspace.”

The two sides hope to announce an agreement to limit certain types of hacking, though people familiar with the negotiations say the talks have been contentious and any deal unveiled this week will probably be modest.

“Cybersecurity is shaping up to be one of those things whose impact is so enormous that it could affect the trajectory of the relationship,” said Wang Fan, director of the Institute of International Relations at the China Foreign Affairs University. Xi and Obama are likely to only reach an agreement in principle or risk “derailing the entire bilateral relation.”

U.S. government agencies and companies are reeling from a string of sophisticated attacks allegedly carried out by the Chinese government or its proxies, including the theft of corporate information and millions of health care and federal personnel records. China denies being involved, saying it is a victim of cyberespionage itself and opposes hacking.

“We are preparing a number of measures that will indicate to the Chinese that this is not just a matter of us being mildly upset,” Obama said Sept. 16. It was his most forceful comment to date and indicates a mounting frustration within the U.S. over what it says is Chinese theft of trade secrets and intellectual property.

Obama said his “hope” is that the U.S., China and other countries can agree to “some basic international framework” governing cybersecurity activities.

One goal is a bilateral agreement embracing a code of conduct put forward by a United Nations working group in June saying that no country should intentionally damage critical infrastructure providing public services, according to current and former government officials with knowledge of the talks who spoke on the condition of anonymity.

Areas where the two governments hope to announce agreement include language restricting attacks on power grids and other vital services and legal cooperation on prosecuting criminal hackers, the officials said.

While such a deal would allow the U.S. “to have a deliverable on cyber,” it would largely be symbolic, said Bonnie Glaser, a senior adviser on China at the Center for Strategic and International Studies in Washington.

Reaching agreement on the problem most vexing the U.S. — Chinese-sponsored hacking of trade secrets and intellectual property from U.S. companies — is seen as much more difficult.

Obama said he wants to put an end to a “government or its proxies engaging directly in industrial espionage and stealing trade secrets, stealing proprietary information from companies.” The Obama administration differentiates between hacking for industrial spying and for traditional intelligence purposes.

“Cyber-enabled espionage that targets personal and corporate information for the economic gain of businesses undermines our long-term economic cooperation, and it needs to stop,” U.S. National Security Advisor Susan Rice said during a speech in Washington on Monday. “We’ll continue to urge China to join us in promoting responsible norms of state behavior in cyberspace.”

Obama also warned that the U.S. could unleash powerful offensive cyberattacks. While the U.S. has more capabilities to carry out cyberattacks, the Chinese likely enjoy an advantage when it comes to disrupting the unclassified networks operating critical infrastructure, according to an analysis released Sept. 14 by the research organization Rand Corp.

“Attacks against a limited set of civilian targets could have significant operational effects, especially if an attack (or its effects) could be sustained,” the report said.

“The United States brings a much better foundation to the battle than China does,” according to the report. “This is likely true in the offensive domain, and it is almost certainly true defensively. The bad news, not surprisingly, is that China’s cyberwarfare capabilities are improving faster, and U.S. efforts cannot slacken.”

In a Wall Street Journal interview on Tuesday, Xi reiterated denials that his government engages in cyberespionage. China was “ready to strengthen cooperation with the U.S. side on this issue,” he said, without elaborating.

“Cybertheft of commercial secrets and hacking attacks against government networks are both illegal,” Xi said. “Such acts are criminal offenses and should be punished according to law and relevant international conventions.”

The U.S. belief that China has developed an organizational infrastructure for accumulating data and distributing it to Chinese companies was highlighted by its accusation last year against five Chinese military officials for stealing trade secrets from companies including Westinghouse Electric Co. and United States Steel Corp.

“The evidence seems to indicate that this is a pretty well-established part of their government machinery,” said Eric Heginbotham, a senior political scientist at Rand Corp.

China may demand the U.S. revoke its indictment of the officers, said Shen Dingli, vice dean of the Institute of International Affairs, Fudan University in Shanghai. For the U.S., that is a “nonstarter” and may make a deal impossible to conclude at the summit, he said.

The Obama administration indicated last month it was considering economic sanctions on Chinese individuals and companies. The Chinese responded by sending Meng Jianzhu, China’s top legal and domestic security official, to Washington for talks with security and intelligence officials, including Rice.

Chinese media cited Meng as saying both sides had reached “an important consensus on combating cybercrimes” and that China would crack down on illegal hacking within its borders.

White House press secretary Josh Earnest described the talks as “pretty blunt.”

“The two sides are still pretty far apart,” said Adam Segal, a cybersecurity expert at the Council on Foreign Relations in New York. “We would have to really see a significant downturn in state-sponsored or state-directed hacking for there to be some sign that the U.S. has gotten what it was hoping for from the summit.”

### 2NC – AT: CFIUS doesn’t review cyber espionage cases

#### Yes they do

Rosenzweig 13 – (Paul Rosenzweig is a Distinguished Visiting Fellow at the Homeland Security Studies and Analysis Institute and serves as a Professorial Lecturer in Law at George Washington University, a Senior Editor of the Journal of National Security Law & Policy, and as a Visiting Fellow at The Heritage Foundation; he is the founder of Red Branch Consulting PLLC, a homeland security consulting company and a Senior Advisor to The Chertoff Group. Mr. Rosenzweig formerly served as Deputy Assistant Secretary for Policy in the Department of Homeland Security; 5/26/13, “Cybersecurity, CFIUS, and the Propose SoftBank Purchase of Sprint-Nextel,” *Lawfare*, <https://www.lawfareblog.com/cybersecurity-cfius-and-propose-softbank-purchase-sprint-nextel>, Accessed 6/27/16, HWilson)

The answer lies in the Committee on Foreign Investment in the United States (CFIUS). CFIUS is an inter-agency committee authorized to review transactions that could result in control of a US business by a foreign person (known as “covered transactions”), in order to determine the effect of such transactions on the national security of the United States. CFIUS operates pursuant to section 721 of the Defense Production Act of 1950, as amended by the Foreign Investment and National Security Act of 2007 and as implemented by Executive Order 11858 (as amended), and regulations at 31 C.F.R. Part 800. The Director of National Intelligence is tasked with conducting an intelligence assessment of the risks posed by certain transactions and reporting to the committee on his findings. His representative sits, ex officio, on the committee and brings a counter-intelligence perspective to its deliberations where appropriate.

If CFIUS determines that the proposed transaction poses a risk of some sort it may prohibit the transaction altogether or, far more frequently, it may enter into a mitigation agreement that puts in place mechanisms and requirements that it deems necessary to ameliorate the risk. Though CFIUS was initially created to focus on the sale of companies that would result in foreign control of defense-critical industries, in the post-9/11 world it has come, as well, to focus on sales that will effect critical infrastructure (such as the sale of port facilities to Dubai Ports World). This focus has, on at least one publicly acknowledged occasion, involved the review of a purchase that implicated cybersecurity concerns.

### 2NC – AT: Other Actors Thump

#### China’s the most important actor in the game

Montopoli 13 – (Brian Montopoli is the national reporter and political analyst for CBSNews.com, 8/7/13, “How Chinese hackers steal U.S. secrets,” *CBS News*, <http://www.cbsnews.com/news/how-chinese-hackers-steal-us-secrets/>, Accessed 7/1/16, HWilson)

But China is "the most active and prolific" state player in the hacking game, according to Ling. "It is a national focus agenda item for the Chinese to be active in this way," he said. "It's not a small group of people who just decided they want to do this on their own accord." While the United States was reticent to specifically accuse China of hacking until relatively recently, the Office of the National Counterintelligence Executive said in 2011 that U.S. firms and cyber-security specialists had reported "an onslaught" of network intrusions from China, and in March President Obama's national security advisor, Tom Donilon, warned of "cyber intrusions emanating from China on an unprecedented scale."

## Negative – BIT Reform CP

### Note

I found this in one of the link cards, so decided to cut it and include it just in case

### 1NC – Counterplan

#### Text:

#### The United States federal government should amend the definition of “covered transaction” to include leases, construction, and additional investments in CFIUS reviews.

#### Solves the aff, but preserves sufficient flexibility to avoid the link to the espionage DA

Stanley 15 – (Mary Ellen Stanley, B.A., University of Richmond (2011); M.A., Baylor University (2013); J.D., Brooklyn Law School (Expected 2016); Editor-in-Chief, Brooklyn Journal of International Law (2015-2016); Fellow, Dennis J. Block Center for the Study of International Business Law (2014-2016); 2015, “From China with Love: Espionage in the Age of Foreign Investment,” Published in *Brooklyn Journal of International Law*, Vol.40, Issue 3, pgs 1033-1079; <http://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1113&context=bjil>, Accessed 6/24/16, HWilson)

Throughout U.S. history, national security has been a paramount concern of the U.S. government. 15 In recent decades, burgeoning technologies and the rise of unconventional acts of terror have heightened fears for the nation’s security. These fears have resulted in the perception of new threats to the nation’s security and a labyrinthine definition of “national security.”16 Conventional acts of espionage––those primarily associated with identifiable persons or groups––have conceptually merged with cybersecurity breaches and industrial espionage.17 The Federal Bureau of Investigation (“FBI”) notably remarked that “[t]he Cold War is not over, it has merely moved to a new arena: the global marketplace.”18 This amalgamation of threats has created a “poisoned climate” in which to balance the nation’s economic prosperity and national security.19 In this environment, cyber-espionage has threatened prominent U.S. businesses, including Home Depot and J.P. Morgan Chase.20 These events illustrate widespread flaws in corporate and government security across the globe.

As globalization accelerates and the world’s largest corporations conduct cross-border transactions with increasing frequency,21 businesses can be victims of espionage, or instead become vessels for espionage through FDI.22 This can occur in two ways: first, when a State-owned or government-connected entity conducts business in the United States; and second, when a foreign entity purchases a U.S. business.23 Foreign ownership of U.S. entities establishes a foreign presence in the United States and enables theft of “American technology, intellectual property, and sensitive information pertaining to critical infrastructure.” 24

While the FBI, Central Intelligence Agency, and National Security Agency address certain security concerns stemming from foreign investments, CFIUS is the government agency charged with preserving this nuanced component of national security.25 CFIUS is an inter-agency committee of the U.S. government26 and is authorized to review transactions that could “result in control of a U.S. business by a foreign person.” 27 CFIUS conducts such reviews to determine whether certain transactions pose national security threats.28 However, this review places an additional burden on CFIUS’s duties as a governmental agency. CFIUS must maintain and protect U.S. national security while simultaneously balancing the business interests of foreign investors.29

While the FBI, Central Intelligence Agency, and National Security Agency address certain security concerns stemming from foreign investments, CFIUS is the government agency charged with preserving this nuanced component of national security.25 CFIUS is an inter-agency committee of the U.S. government26 and is authorized to review transactions that could “result in control of a U.S. business by a foreign person.” 27 CFIUS conducts such reviews to determine whether certain transactions pose national security threats.28 However, this review places an additional burden on CFIUS’s duties as a governmental agency. CFIUS must maintain and protect U.S. national security while simultaneously balancing the business interests of foreign investors.29

CFIUS’s secretive evaluations—and its power—have become an increasingly contested political issue, both domestically and abroad.30 In the United States, these debates have garnered significant legislative responses. For example, Congresswoman Rosa DeLauro recently proposed legislation to amend the CFIUS review process to include an evaluation of whether the transaction results in a “net benefit” to the United States.31 In the international arena, as a response to CFIUS reviews, nations such as the People’s Republic of China (“China”) have instituted their own protectionist regimes.32 Critics of CFIUS assert a variety of complaints, alleging both inaction and prejudiced reviews.33 The correct balance must be struck, between ensuring the nation’s security and promoting FDI, if all the foregoing concerns are to be addressed.

This Note argues that the U.S. government should neither explicitly define “national security” in the context of CFIUS reviews, nor expand its definition to include a “net-benefit” or economic review, as proposed by Congresswoman DeLauro’s legislation.34 Rather, the definition of “national security” should remain undefined to allow the government to adapt its security reviews to unpredictable and evolving threats. Alternatively, the type of “covered transaction[s]” that CFIUS has the power to review should be amended. CFIUS jurisdiction should not hinge upon traditional, corporate law distinctions that define control only in terms of mergers, acquisitions, and takeovers. Rather, CFIUS’s jurisdiction should maintain a more equitable approach to other types of nontraditional control that could pose a security threat.35 An amended definition of a “covered transaction” should include leases, construction, and additional investments. 36 A more inclusive definition that directs the Committee’s focus to examine the substance and effect of transactions, rather than merely the structure, will provide a more comprehensive review of FDI. These amendments will not only eliminate loopholes in the enacting legislation, but also increase the quality and integrity of CFIUS national security reviews. Additionally, such amendments will nurture the United States’ presence in international markets by not further discouraging FDI with a more economically focused and intrusive national security review.

### 2NC – AT: No Accountability

#### Congressional checks ensure accountability and effectiveness

Stanley 15 – (Mary Ellen Stanley, B.A., University of Richmond (2011); M.A., Baylor University (2013); J.D., Brooklyn Law School (Expected 2016); Editor-in-Chief, Brooklyn Journal of International Law (2015-2016); Fellow, Dennis J. Block Center for the Study of International Business Law (2014-2016); 2015, “From China with Love: Espionage in the Age of Foreign Investment,” Published in *Brooklyn Journal of International Law*, Vol.40, Issue 3, pgs 1033-1079; <http://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1113&context=bjil>, Accessed 6/24/16, HWilson)

CFIUS is an inter-agency committee for which the Secretary of the Treasury serves as chairperson.51 Notices are “received, processed, and coordinated” by the CFIUS Staff Chairperson.52 Additional members of the Committee include the heads of the Department of Justice, Department of Homeland Security, Department of Commerce, Department of Defense, Department of State, Department of Energy, Office of the U.S. Trade Representative, and Office of Science and Technology Policy.53 The CFIUS review process is structurally protected from politicization by Congress, because the oversight powers of Congress are retrospective only.54 Nevertheless, CFIUS still maintains ties to bipartisan politics.55 To maintain accountability for CFIUS actions, Section 721 requires CFIUS to submit an annual report56 to Congress detailing its reviews of international business transactions.57 Additionally, the Committee must deliver a certified report to Congress upon completing an investigation–– and the lead agency must transmit the contents and results of the investigation to members of Congress58––unless the matter was sent to the President for decision.59 Some argue CFIUS has evolved into a “congressional notification service” due to the fact that Congress has responded to economic crises by expanding its supervision of CFIUS.60

## Affirmative

### 2AC – Non-Unique – Espionage Now

#### Non-unique – Chinese economic espionage is high now and thousands of companies have been hit – also proves no link

Stahl 16 – (Lesley Rene Stahl is an American television journalist. She has spent most of her career with CBS News, having been affiliated with that network since 1972; since 1991, she has reported for CBS' 60 Minutes; the article cites interviews with her and John Carlin, assistant attorney general for National Security with responsibility for counterterrorism, cyberattacks and increasingly economic espionage, Daniel McGahn, the head of American Superconductor, and Dmitri Alperovitch and George Kurtz, cofounders of a computer security firm called CrowdStrike; 1/17/16, “The Great Brain Robbery,” *CBS News: 60 Minutes*, <http://www.cbsnews.com/news/60-minutes-great-brain-robbery-china-cyber-espionage/>, Accessed 6/30/16, HWilson)

Economic espionage sponsored by the Chinese government is costing U.S. corporations hundreds of billions of dollars and more than two million jobs

If spying is the world's second oldest profession, the government of China has given it a new, modern-day twist, enlisting an army of spies not to steal military secrets but the trade secrets and intellectual property of American companies. It's being called "the great brain robbery of America."

The Justice Department says that the scale of China's corporate espionage is so vast it constitutes a national security emergency, with China targeting virtually every sector of the U.S. economy, and costing American companies hundreds of billions of dollars in losses -- and more than two million jobs.

John Carlin: They're targeting our private companies. And it's not a fair fight. A private company can't compete against the resources of the second largest economy in the world.

John Carlin is the assistant attorney general for National Security with responsibility for counterterrorism, cyberattacks and increasingly economic espionage.

John Carlin: This is a serious threat to our national security. I mean, our economy depends on the ability to innovate. And if there's a dedicated nation state who's using its intelligence apparatus to steal day in and day out what we're trying to develop, that poses a serious threat to our country.

Lesley Stahl: What is their ultimate goal, the Chinese government's ultimate goal?

John Carlin: They want to develop certain segments of industry and instead of trying to out-innovate, out-research, out-develop, they're choosing to do it through theft.

All you have to do, he says, is look at the economic plans published periodically by the Chinese Politburo. They are, according to this recent report by the technology research firm INVNT/IP, in effect, blueprints of what industries and what companies will be targeted for theft.

John Carlin: We see them put out the strategic plan, and then we see actions follow that plan. We see intrusion after intrusion on U.S. companies.

Lesley Stahl: Do you have a number of U.S. companies that have been hit?

John Carlin: It's thousands of actually companies have been hit.

Lesley Stahl: Thousands of U.S. companies?

John Carlin: Of U.S. companies.

### ---XT: Non-Unique – Espionage Now

#### Cyber espionage is coming now through avenues external to CFIUS and will only get worse

Cheng 16 – (Dean Cheng is a senior research fellow in The Heritage Foundation’s Asian Studies Center, 3/18/16, “Here's Why China's Cyber Strategy Should Have America Worried,” *The National Interest*, <http://nationalinterest.org/blog/the-buzz/heres-why-chinas-cyber-strategy-should-have-america-worried-16245>, Accessed 7/1/16, HWilson)

Chinese activities in cyberspace regularly garner a great deal of attention. Chinese hackers have been accused of stealing millions of records from U.S. government databases, such as the Office of Personnel Management, as well as various corporations.

But too often, the focus is on the individual attack, rather than understanding the larger context. This leaves us playing whack-a-mole when trying to deal with Chinese cyber espionage efforts.

In fact, Chinese leadership sees information as inextricably linked to not only the broader national interest, but also to regime survival.

The People’s Republic of China is interested in improving its “comprehensive national power,” the combination of economic, military, political, social, and cultural factors that together reflect national capabilities. In the information age, information is the vital resource that enables all types of power.

At the same time, however, the free flow of information constitutes a dire potential threat to Chinese Communist Party rule. China has emplaced the “Great Firewall of China” and deployed an army of censors numbering in the tens, or even hundreds of thousands, to limit the informational threat to the regime.

But this is insufficient to allay Beijing’s concerns. Ideally, China must control and influence all information flowing to China, which means shaping and molding the international structures that manage that information flow.

China is interested in setting the global norms for cyberspace, but in ways that fundamentally challenge and contradict the free flow of information that the United States has long championed.

So, Chinese cyber actions should be seen as part of a broader effort to secure the means for China to sustain its growth in power (made more urgent by the slowing of the Chinese economy), while also defending the People’s Republic of China, and especially, the Chinese Communist Party’s rule.

The recently announced Chinese military reforms highlight the importance that Chinese leadership now accords information. Among the reforms is the creation of a new service, the PLA Strategic Support Force.

This innocuously named entity is, in fact, China’s information warfare forces, now grouped into a single service. The PLA Strategic Support Force reportedly has responsibility for China’s space forces, electronic warfare forces, and network warfare forces.

As a careful student of America’s wars, from Operation Desert Shield/Desert Storm against Iraq to Operation Inherent Resolve against the Islamic State, China knows how much the American military depends on easy access to information to fight its wars.

Given the importance accorded information in China’s own conceptions of future wars (termed “local wars under informationized conditions”), the PLA Strategic Support Force is sure to have a central role in any future conflict, targeting an adversary’s space systems, electronic systems, and computer networks and information systems.

### 2AC – Status Quo Solves

#### Espionage declining – most recent – cites government officials

Volz 16 – (Dustin Volz is a DC-based journalist for Reuters covering cybersecurity and surveillance policy. Previously Dustin was a staff correspondent for National Journal, where he covered tech policy; 6/28/16, “Chinese economic cyber-espionage is diminishing, says U.S. official,” <http://www.reuters.com/article/us-cyber-china-idUSKCN0ZE1S8>, Accessed 6/29/16, HWilson)

U.S. Assistant Attorney General John Carlin said on Tuesday that Chinese hacking activity appears to have declined since the Chinese government vowed last September to stop supporting the hacking of U.S. trade secrets.

The assertion supports findings released earlier this month from cyber security firm FireEye that breaches attributed to China-based groups had plunged by 90 percent in the past two years.

"Generally, people have seen a change in activity," Carlin said at the Center for Strategic and International Studies think tank in Washington.

But "there is debate about how long lasting" the apparent reduction in activity will be, Carlin said, adding that the private sector and U.S. intelligence officers were likely better positioned to assess hacking trends.

Carlin said that agreements on hacking activity with China and among the Group of 20 nations, both announced last year, were important to developing uniform international cyber norms.

### ---XT: Status Quo Solves

#### Recent US-China agreement solves

Zetter 15 – (Kim Zetter is an award-winning, senior staff reporter at Wired covering cybercrime, privacy, and security; 9/25/16, “US and China Reach Historic Agreement on Economic Espionage,” *Wired*, <https://www.wired.com/2015/09/us-china-reach-historic-agreement-economic-espionage/>, Accessed 6/29/16, HWilson)

THE US AND China have been sparring for years over allegations that the Chinese government has been hacking US companies to steal trade secrets. Today the two announced a historic agreement that, at least on its face, puts an end to this kind of spying.

President Obama said during a press conference today with visiting Chinese President Xi Jinxing, that the two nations have reached a “common understanding” to not conduct or support cyber espionage and intellectual property theft for the purposes of commercial gain.

“I raised, once again, our rising concerns about growing cyber threats to American companies and American citizens,” Obama said. “I indicated that it has to stop… We have agreed that neither the US or the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage. We’ll work together and with other nations to promote other rules of the road.”

The US has long insisted that it does not spy on other nations for purposes of economic or commercial gain, and that it does not pass information obtained through intelligence operations onto US companies in order to give them a competitive advantage in the marketplace.

China, however, has long been suspected of spying on companies in the US defense, tech, and energy sectors in order to advance Chinese businesses and innovations. President Xi did not publicly acknowledge the activity but agreed with Obama at the press conference that “confrontation and friction are not the right choice for both sides.” He also reportedly agreed to become more cooperative in responding to US law enforcement requests in seeking aid to track down cybercriminals in China.

Obama said the US would be watching closely to determine whether “words are followed by actions” and would not hesitate to use sanctions and other “tools” against China for such activity.

China, of course, has been implicated in the recent massive hack against the Office of Personnel Management, which involved the theft of sensitive data on some 21 million people, including the fingerprint records of more than 5 million federal workers, many of whom hold security clearances and use their fingerprints to gain access to secured facilities.

This, however, is not the kind of hacking that would be barred under the new agreement, since it falls under traditional categories of nation-state spying. The agreement barring economic spying refers to other attacks, such as ones against Google and some 30 other tech companies in 2010 that aimed to steal their source code, as well as the kinds of breaches allegedly conducted by five Chinese hackers whom the US government indicted last year. All five, who are said to be associated with China’s People’s Liberation Army, are accused of stealing information from six companies in the energy, metals, and manufacturing industries.

The FBI said in a report released earlier this year that economic espionage cases in the US surged 53 percent in 2014, and that China was responsible for most of it.

Congressman Jim Langevin (D-Rhode Island), a senior member of the House Armed Services and Homeland Security Committees, expressed cautious optimism at the news.

“This agreement represents important, substantive progress in the relationship between the U.S. and China,” he said in a statement. “For too long, Chinese hackers—both governmental and criminal—have exploited American companies by stealing their hard-won intellectual property and using it to further their own economic interests. This accord clarifies that so-called ‘economic espionage’ is not espionage but theft and that it has no place in 21st century dealings between states.”

He noted, however, that he remains skeptical about the Chinese commitment to carry out the agreement.

“I believe that the threat of sanctions brought President Xi to the negotiating table, and President Obama must make clear to his counterparts that sanctions will be levied on rogue actors in cyberspace.”

#### International cyber-norms coming now

Dahl 15 – (Matt Dahl is Manager of Global Threat Intelligence and Legal Counsel for the cybersecurity technology firm, CrowdStrike; 12/4/15, “Agreements on Commercial Cyber Espionage: An Emerging Norm?,” *Lawfare*, [https://www.lawfareblog.com/agreements-commercial-cyber-espionage-emerging-norm Accessed 6/27/16](https://www.lawfareblog.com/agreements-commercial-cyber-espionage-emerging-norm%20Accessed%206/27/16), HWilson)

When the U.S. and China reached an agreement in late September not to engage in commercially motivated cyber espionage it was viewed as a significant step forward in cybersecurity relations between the two countries. A few weeks later, China reached the same deal with the U.K., and soon after Germany announced that it would likely enter into a similar agreement. Suddenly, the progress initially made between the U.S. and China, took on global significance as governments representing four of the top five economies in the world addressed the issue of cyber espionage carried out for commercial gain. The rapid succession of these deals raises an interesting possibility: we may be moving towards the formation of international law norms against economically motivated cyber espionage.

[Note: As a primer, “The Nature of International Law Cyber Norms” is an excellent general background on the existence and formation of norms in international law and how they are formed.]

There is currently little by way of international law norms pertaining to activities in cyberspace; in fact, there is little international law of any type applicable to the domain. Generally, norms arise from either treaties or customary international law. The agreements that the U.S. and U.K. have reached—and Germany hopes to reach—with China are not treaties because the agreements do not create any legally binding rights between the parties. In particular, the U.S.-China deal cannot constitute a treaty because it was made without the “advice and consent” of the Senate, as constitutionally required. It is possible, however, that these agreements lay the foundation for the formation of customary law against commercially motivated cyber espionage.

Customary international law comprises a set of general practices which are accepted as law by the international community. Customary laws form when states conduct themselves in a certain manner over an extended period of time and out of a sense of legal obligation. This standard for formation is, admittedly, non-specific. There are not bright-line rules governing how long a practice must occur before it becomes a norm. Although often customary norms take many years to emerge, examples of rapidly crystallizing norms do exist, such as those governing the law of space. This might indicate that norms potentially emerge more quickly in relatively new domains like cyberspace.

So, will these agreements prohibiting commercially motivated cyber espionage form the foundation for a new norm recognized under international law? That depends on whether states decide to abide by them. The agreements themselves are not necessary for the ultimate formation of a norm prohibiting commercial espionage; what is necessary is for states to not engage in commercially motivated cyber espionage for a sufficient period of time. But to the extent the agreements indicate the actual intention of states not to engage in this type of espionage, they represent the first steps towards the formation of a norm under customary international law.

Just this week, U.S. and Chinese officials met in Washington to discuss cybersecurity issues as part of the deal reached in September. Media reports indicate the meetings might be seen as a movement towards the establishment of a norm in this area. And perceptions that norms are developing can be self-reinforcing; the perception acts as the impetus for more states enter into similar agreements against commercial cyber espionage or to simply refrain from undertaking the behavior, and thus the norm is more likely to ultimately develop.

#### Status quo solves – China’s economic espionage is going down now

Menn and Finkle 16 – (Joseph Menn is an author, speaker and investigative reporter specializing in technology issues for Reuters, having previously worked for the Financial Times and the Los Angeles Times; Jim Finkle is a long-time journalist with Reuters covering issues of cybersecurity and privacy; 6/21/16, “Chinese economic cyber-espionage plummets in U.S.: experts,” <http://www.reuters.com/article/us-cyber-spying-china-idUSKCN0Z700D>, Accessed 6/28/16, HWilson)

The Chinese government appears to be abiding by its September pledge to stop supporting the hacking of American trade secrets to help companies there compete, private U.S. security executives and government advisors said on Monday.

FireEye Inc, the U.S. network security company best known for fighting sophisticated Chinese hacking, said in a report released late Monday that breaches attributed to China-based groups had plunged by 90 percent in the past two years. The most dramatic drop came during last summer's run-up to the bilateral agreement, it added.

FireEye's Mandiant unit in 2013 famously blamed a specific unit of China's Peoples Liberation Army for a major campaign of economic espionage.

Kevin Mandia, the Mandiant founder who took over last week as FireEye chief executive, said in an interview that several factors seemed to be behind the shift. He cited embarrassment from Mandiant's 2013 report and the following year's indictment of five PLA officers from the same unit Mandiant uncovered.

### 2AC – CFIUS Fails

#### CFIUS fails – their uniqueness evidence says that attacks are happening now – that proves that CFIUS is ineffective or the Chinese will spy through other methods

#### CFIUS doesn’t solve anything – it gets circumvented – their ev

Stanley 15 – (Mary Ellen Stanley, B.A., University of Richmond (2011); M.A., Baylor University (2013); J.D., Brooklyn Law School (Expected 2016); Editor-in-Chief, Brooklyn Journal of International Law (2015-2016); Fellow, Dennis J. Block Center for the Study of International Business Law (2014-2016); 2015, “From China with Love: Espionage in the Age of Foreign Investment,” Published in *Brooklyn Journal of International Law*, Vol.40, Issue 3, pgs 1033-1079; <http://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1113&context=bjil>, Accessed 6/24/16, HWilson)

A foreign entity’s mere presence could have severe implications for national security. Thus, these additional transactions should be reviewed under the same standards as the more traditional covered transactions. Furthermore, these additional transactions allow canny investors to evade CFIUS review by restructuring transactions that would be covered under the current legislation into leases, construction, and additional investments, or into other nontraditional investments such as greenfield investments.257 Since the legislation does not have an “anti-circumvention clause” 258 or a focus on the substance of the transaction, as seen in the Chinese Model, foreign investors are able to use alternative investment structures to sidestep CFIUS reviews.259 Not requiring approvals of such alternative transactions sets a dangerous precedent for national security. As a result, the CFIUS review process must look beyond the form of a transaction and review both the substance of a transaction and its effects.

### 2AC – Aff Solves

#### The aff solves the impact – the only way to ensure that espionage is limited is increasing relations and co-operation – i.e. the plan

Gordon 15 – (Nicholas Gordon is a researcher at the Global Institute For Tomorrow in Hong Kong. He has an MPhil from Oxford in International Relations and a BA from Harvard. His writing has also appeared in The South China Morning Post, The Diplomat, China Daily and Caixin. A version of this review was originally published in the Asian Review of Books; 9/29/15, “Review: China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain,” <http://thediplomat.com/2015/09/review-china-and-cybersecurity-espionage-strategy-and-politics-in-the-digital-domain/>, Accessed 6/29/16, HWilson)

The agreement between the United States and China to limit cyberespionage of intellectual property for commercial gain, announced on September 25, caps a tense debate over Chinese activities in cyberspace. Over the past several months, American officials had routinely called high-profile breaches of American digital networks, such as the hacking of the Office of Personnel Management, state-sanctioned espionage. This fed a belief, held by both American and Chinese officials, that China’s “cyberwarfare doctrine” is a way to balance America’s superior conventional capabilities.

Jon R Lindsay, Tai Ming Cheung, and Derek S Reveron have compiled a timely volume of academic papers detailing, in their words, how China both generates and copes with Internet insecurity through close attention to its domestic institutions and processes.

This multifaceted book discusses the doctrines, motives, purposes, and capabilities of Chinese activities in cyberspace, internal and external. The chapters authored by Chinese writers, including one current member of the People’s Liberation Army, are especially illuminating. Particularly striking are their attempts to create new terms to describe this new sphere of geopolitical activity, and their overall optimism over the possibility of international management of cyberspace.

The inclusion of the Chinese authors is not just even-handed but necessary, for this is primarily a book about China. The American writers largely view the United States as a victim of Chinese cyberespionage, neglecting in large part the other prominent entity: the U.S. National Security Agency. American cyber-activity is discussed mostly in passing by the book’s American authors, though the Chinese authors as well as the editors ensure that the contradictions inherent in American protestations are mentioned.

The official position of the United States, according to Professor Fred Cate, one of the volume’s concluding authors, is that it only conducts cyber operations against government for military and other commercial information, while the Chinese are hacking businesses for trade secrets and commercial information.

The strange corollary to this argument [is] that commercial secrets are somehow more valuable than military information. It also creates a distinction between the private and public spheres that that is increasingly blurry given how often corporate success is seen as a part of national interest. Nor, finally, does this distinction have any basis in fact. Edward Snowden’s revelations have revealed that the NSA has targeted Huawei, Hong Kong-based universities, and foreign trade delegations.

This has made the American argument, continues Cate, “a tough sell.” He quotes a former Department of Defense official as saying

… the Huawei revelations are devastating rebuttals to hypocritical U.S. complaints about penetration of U.S. networks, and also make USG protestations about not stealing intellectual property to help U.S. firms’ competitiveness seem like the self-splitting hairsplitting that it is.

Philosophy aside, the practical difficulty in controlling cyberespionage, as shown by both American and Chinese activity, is that it very hard to sanction. Both traditional and cyberespionage break the target country’s laws, but only the former requires (in most cases) someone to be physically inside a country’s territory and thereby subject to apprehension. Even if law enforcement could identify precisely who instigated a hack, actual arrests are rarely possible. Thus, domestic sanctions are largely meaningless.

This is of course a function of the Internet itself, which allows action at distance, and is not a characteristic of cyberespionage per se. American websites pushing information through the Great Firewall may in practice be in violation of local Chinese censorship laws, yet China can do little but block access to those websites. This issue also occurs between allies: France’s data-privacy watchdog has told Google and other Internet firms that, in order to execute Europe’s “right to be forgotten,” they need to scrub offending links from all their websites, and not just their European versions. Of course, without erecting a China-style firewall, there is little France can practically do.

The editors’ conclude that

… the United States and China, or any other advanced industrial countries [sic] for that matter, will not be able to separate cybersecurity from their diplomatic relations.

Cyberespionage, furthermore

is simply too essential a tool for China’s economic development and political stability strategy and for the national security strategy of the United States

for either country to expect the other to limit its activity.

Cyberespionage and its variants therefore become an important avenue for inter-state competition, though its extent, threat and usefulness remain subject to actual international conditions.

The editors provide a useful two-by-two matrix in their final chapter that best illustrates the possible outcomes. One dimension asks whether the international environment is collaborative or combative; the second asks whether the threats posed by cyberspace are limited or severe. A collaborative environment is more able to manage the threats posed by cyberspace; severe threats would lead to the development of new norms and rules governing cyberspace. However, a competitive environment leads to different outcomes: mild threats leads to “contested cyberspace”, while severe threats leads to cyberwarfare.

The question thus becomes whether the international environment is collaborative or competitive, and whether threats are mild or severe. These determinations are clearly easier listed than evaluated, and they require a knowledge of local institutions in both the United States and China, the possibility of cooperation, and whether either side feels the other’s cyberactivities represent an “existential threat”.

There are a few hopeful indications that things may not be as bad as pessimists believe. First, despite the “cloak-and-daggers” vibe in many general discussions around cyberespionage, the researchers have drawn intelligent and well-thought out conclusions using publicly-available data: the chapter detailing the locations of China’s information-warfare groups and the state-owned companies they are attached to was compiled using publicly-accessible websites.

There is also room for cooperation between China and the United States, or at least an understanding of what is broadly unacceptable. Cate argues that a focus on China is ill-advised, as it

contributes to US policymakers losing sight of the broad range of cyberthreats and their many sources, which include, but certainly are not limited to, China.

If cybersecurity really presents such broad threats, it may be that Washington and Beijing can agree on some solutions. Both countries have promised not to target “critical infrastructure” (however that is defined) during peacetime, and have pledged to pursue cybercrime more vigilantly within their own territories. In addition, as China develops further, it may reach a point where allowing unchecked cyberespionage presents more costs than benefits, pushing Beijing to support more international management. It remains to be seen how these agreements develop, yet while it seems that the odds are that cybersecurity will become a significant source of tension between Beijing and Washington, the editors note (with some surprise) that Chinese authors are much more optimistic that cyberspace can be managed than are the American authors.

The editors’ framework is helpful for evaluating the probability of each outcome. If the international environment is cooperative, the results will be largely benign; if anything, more severe threats will make an international solution more likely. In contrast, a more competitive environment makes the danger posed by cyberspace becomes far more important, making the difference between a contested, but ultimately peaceful, cyberspace (akin, perhaps, to Cold War mistrust) and outright “cyberwarfare.”

Cyberspace is both new and complicated, even lacking in many instances the questions to be asked when analyzing the issue. China and Cybersecurity is a step towards providing them. Are threats perceived to be existential, or merely troublesome? How conducive are both countries to international management? Are countries able to close themselves off from the global Internet without suffering disproportionate consequences, as China has partially done? With these in mind, one can begin to evaluate whether these new activities is really as threatening as the pessimists believe, or whether it remains a significant, but not dangerous, nuisance.

### 2AC – CFIUS Not Key

#### Non-unique and no link – Chinese hacking is successful now and CFIUS isn’t key – hackers will just take other routes

Montopoli 13 – (Brian Montopoli is the national reporter and political analyst for CBSNews.com, 8/7/13, “How Chinese hackers steal U.S. secrets,” *CBS News*, <http://www.cbsnews.com/news/how-chinese-hackers-steal-us-secrets/>, Accessed 7/1/16, HWilson)

To steal the designs for America's advanced weapons systems, as Chinese hackers are alleged to have done by in a confidential report prepared for the Pentagon, you don't necessarily have to break into classified Department of Defense systems.

Many of America's military secrets can be stolen by exploiting the networks over which unclassified information is shared by military contractors and subcontractors. While these contractors, like the government, have improved their cyber-security over the past decade, many still do not have systems in place to quickly discover whether a hacker in Beijing, or elsewhere, is harvesting information off the computer of a staffer in Virginia, according to cyber-security experts interviewed for this story.

On Monday, the Washington Post reported that Chinese hackers are believed to have stolen the designs for "more than two dozen major weapons systems," potentially weakening the U.S. military advantage over China. While we don't know precisely how the information was accessed, cyber-security experts say it did not necessarily come from the Department of Defense itself.

"I just don't think that's necessary," said Richard Bejtlich, the Chief Security Officer for cyber-security company Mandiant. "You can get what you need from the contractors."

While no computer networks are impenetrable, federal agencies like the FBI, DOD and NSA devote significant resources to guard their computer networks, and also have in place rules to protect sensitive data. Many of the contractors who build parts for U.S. weapons systems, however, do not have that level of resources. That makes them more vulnerable to attacks from hackers in China and elsewhere, who often use sophisticated "spear phishing" attacks to infiltrate a system and harvest data. By piecing together stolen information from various contractors, hackers can recreate U.S. systems even if they don't have the entire design in one place.

James E. Harris Jr., a senior specialist for cyber-security at Obsidian and former FBI cyber-division official, said that while "we may protect a final design," important aspects of it go to vendors for fabrication. Those vendors may order parts from another supplier or subcontractor, potentially exposing sensitive information to a network with a lower level of security than the contractor itself. "Nobody produces anything from soup to nuts," he said.

While spear-phishing attacks involve email, they are far more sophisticated than the clumsy, implausible email appeals you've most likely gotten from an alleged Nigerian prince or other scammer. A hacker may spoof or break into the email of a friend or colleague - they might use Facebook to figure out your connections - and send along a link or attachment that downloads malware onto your computer; when you click it installs malware can then record your keystrokes, turn on your camera, and go through your windows registry for sensitive information. These emails are often well-written and believable: The National Association of Manufacturers recently received an email ostensibly from a Bloomberg reporter with a link to an Excel spreadsheet relevant to a story. The email had actually come from Chinese hackers seeking proprietary information.

Indeed, U.S. weapons systems are just one of the many targets of hackers, who are equally (if not more) interested in industrial secrets and intellectual property. And the Chinese government is far from the only game in town: There are organized criminal gangs, other state actors and other autonomous groups constantly trying to break into systems. Christopher Ling, executive vice president at Booz Allen Hamilton focusing on military intelligence and cyber-security, said that Russia and Israel are among the countries (along with the United States) that have excelled in the "cat and mouse" game of cyber-warfare, though he added that there is now a black market for sophisticated malware that allows less sophisticated nations to mount serious attacks. And the threat isn't just to military and industrial secrets: Some hackers are also interested in terrorism, with the Department of Homeland Security reporting 198 attacks on critical U.S. infrastructure in fiscal year 2012.

### ---XT: CFIUS Not Key

#### Alt cause – China’s successfully using human intel for theft – makes the impact inevitable

Aid 15 – (Matthew M. Aid is an American military historian and author. He is working on signal intelligence and the history of the National Security Agency, 10/21/15, “Chinese HUMINT Spying in U.S. and Elsewhere Continues Unabated,” <http://www.matthewaid.com/post/131614390416/chinese-humint-spying-in-us-and-elsewhere>, Accessed 7/1/16, HWilson)

In early October 2015 a Chinese businessman (Xiwen Huang) was indicted in the United States for stealing trade secrets from American companies as well as the U.S. government over a ten year period. Huang was caught in part because he and Chinese firms are becoming bolder in how they exploit stolen software, trade secrets and other technology. Often Chinese will describe their espionage feats in print (almost always in Chinese only) and that is becoming more common. For example one of the most damaging pieces of evidence against was a detailed description of his activities Hwang sent home via email. He even gave this account a title; “Trip of Dream Realization” apparently with the intention of later expanding it into a magazine article or book. The article was also a detailed confession of theft of trade secrets and other intellectual property between 2004 and 2014. Huang was arrested in May 2015 on one of his trips back to the United States from his new home (and job) in China.

Since 2012 most American officials have come to openly admit that a whole lot of American military and commercial technical data has been stolen via Chinese Internet espionage efforts as well as more conventional methods like Huang used. The Americans are not providing details of exactly how they collected all the evidence, but apparently it is pretty convincing for many American politicians and senior officials who had previously been skeptical.

It’s no secret that Chinese intelligence collecting efforts since the late 1990s have been spectacularly successful. As the rest of the world comes to realize the extent of this success, there is a building desire for retaliation. What form that payback will take remains to be seen. Collecting information, both military and commercial, often means breaking laws and hacking back at the suspected attackers will involve even more felonies. China has broken a lot of laws. Technically, China has committed acts of war because of the degree to which it penetrated military networks and carried away copies of highly secret material. The U.S., and many other victims, has been warning China there will be consequences. As the extent of Chinese espionage becomes known and understood, the call for “consequences” becomes louder.

China has always tried to conceal its espionage efforts. Not just denying anything and everything connected to its hacking and conventional spying but also by taking precautions. But as their success continued year after year, some of the Chinese hackers and spies became cocky and sloppy. At the same time, the victims became more adept at detecting Chinese efforts and tracing them back to specific Chinese government organizations or non-government hackers inside China.

Undeterred, China has sought to keep its espionage effort going and has even expanded operations. For example, since 2008 China has opened National Intelligence Colleges in many major universities. In effect, each of these is an “Espionage Department” where, each year, several hundred carefully selected applicants are accepted in each school, to be trained as spies and intelligence operatives. China has found that espionage is an enormously profitable way to steal military and commercial secrets and rewards those who have talent and make a career of it. The Internet based operations, however, are only one part of China’s espionage efforts.

While Chinese Cyber War operations in this area get a lot of publicity, the more conventional spying brings in a lot of stuff that is not reachable on the Internet. One indicator of this effort is the fact that American counter-intelligence efforts are snagging more Chinese spies. This is partly due to increased spying effort by China, as well as more success by the FBI and CIA. All this espionage, in all its forms, has played a large part in turning China into one of the mightiest industrial and military powers on the planet. China is having a hard time hiding the source of the new technologies they are incorporating into their weapons and commercial products. Many of the victims initially had a hard time accepting the fact that the oh-so-eager (to export) Chinese were robbing their best customers of intellectual property on a grand scale. Now Western firms are a lot more wary about dealing with the Chinese.

China has been getting away with something the Soviet Union never accomplished, stealing Western technology and then using it to move ahead of the West. The Soviets lacked the many essential supporting industries found in the West (largely founded and run by entrepreneurs) and was never able to acquire all the many pieces needed to match Western technical accomplishments. Soviet copies of American computers, for example, were crude, less reliable, and less powerful. It was the same situation with their jet fighters, tanks, and warships.

China gets around this by making it seemingly profitable for Western firms to set up factories in China, where Chinese managers and workers can be taught how to make things right. At the same time, China allows thousands of their best students to go to the United States to study. While many of these students will stay in America, where there are better jobs and more opportunities, some will come back to China and bring American business and technical skills with them. Finally, China energetically uses the “thousand grains of sand” approach to espionage. This involves China trying to get all Chinese going overseas, and those of Chinese ancestry living outside the motherland, to spy for China, if only a tiny bit.

This approach to espionage is nothing new. Other nations have used similar systems for centuries. What is unusual is the scale of the Chinese effort, and that makes a difference. Supporting it all is a Chinese intelligence bureaucracy back home that is huge, with nearly 100,000 people working just to keep track of the many Chinese overseas and what they could, or should, be trying to grab for the motherland. This is where many of the graduates of the National Intelligence College program will work.

It begins when Chinese intelligence officials examine who is going overseas and for what purpose. Chinese citizens cannot leave the country, legally, without the state security organizations being notified. The intel people are not being asked to give permission. They are being alerted in case they want to have a talk with students, tourists, or business people before they leave the country. Interviews are often held when these people come back as well.

Those who might be coming in contact with useful information are asked to remember what they saw or bring back souvenirs (legal or otherwise). Over 100,000 Chinese students go off to foreign universities each year. Even more go abroad as tourists or on business. Most of these people were not asked to actually act as spies but simply to share, with Chinese government officials (who are not always identified as intelligence personnel), whatever information they obtained. The more ambitious of these people are getting caught and prosecuted. But the majority are quite casual and individually bring back relatively little and are almost impossible to catch.

Like the Russians, the Chinese are also employing the traditional methods, using people with diplomatic immunity to recruit spies and offering cash, or whatever, to get people to sell them information. This is still effective and when combined with the “thousand grains of sand” methods brings in a lot of secrets. The final ingredient is a shadowy venture capital operation (sometimes called Project 863) that offers money for Chinese entrepreneurs who will turn the stolen technology into something real. No questions asked, if you can get back to China with the secrets, you are home free and potentially very rich.

#### Chinese hackers are pursuing alternate types of hacking

Zetter 16

(Kim, 06.14.16, REVEALED: YET ANOTHER GROUP HACKING FOR CHINA’S BOTTOM LINE, <https://www.wired.com/2016/06/revealed-yet-another-chinese-group-hacking-countrys-economic-bottom-line/>, JZG)

IN THE WORLD of cyberespionage, the Chinese are king. More nation-state attacks are attributed to it than any other country. Though the assumption has been that the motive behind most of this spying was to gain a competitive advantage for Chinese companies, there had not been much proof. Until now. A new espionage campaign attributed to China shows an almost one-to-one correlation between the breaches and China’s economic interests. The group, discovered last November by the Dutch security firm Fox-IT and dubbed Mofang, has struck more than a dozen targets in various industries and countries since at least February 2012, and is still active. Mofang has targeted government agencies in the US, military agencies in India and Myanmar, critical infrastructure in Singapore, research and development departments of automotive companies in Germany, and the weapons industry in India. But one campaign in particular, conducted in relation to business dealings in Myanmar’s Kyaukphyu special economic zone, provides clues about the attackers’ motives. In that attack, Mofang targeted a consortium overseeing decisions about investments in the zone, where China’s National Petroleum Corporation hoped to build an oil and gas pipeline. “It’s a really interesting campaign to see where initial investments by a China state-owned company [appeared to drive the breaches],” says Yonathan Klijnsma, senior threat intelligence analyst with Fox-IT. “Either they were afraid of losing this investment or they just wanted more [business opportunities].” Finding Mofang Fox-IT discovered the group after uncovering some of its malware on VirusTotal, a free online service owned by Google that aggregates more than three dozen antivirus scanners made by Symantec, Kaspersky Lab, F-Secure and others. Researchers, and anyone else who finds a suspicious file on their system, can upload the file to the site to see if any of the scanners tag it as malicious. Fox-IT uncovered two primary tools the group uses: ShimRat (a remote access trojan) and ShimRatReporter (a tool for conducting reconnaissance). The malware is custom tooled for each victim, which allowed Fox-IT to identify targets in cases where the victim’s name appeared in email documents the attackers used. Unlike many nation-state hacks attributed to China, the Mofango group doesn’t use zero-day exploits to get into systems but instead primarily relies on phishing attacks that direct victims to compromised web sites where the malware downloads to their system using already known vulnerabilities. The group also hijacks antivirus products to run their malware, so that if a victim looks at the list of processes running on their system, it looks like a legitimate antivirus program is running when really it’s malware. The researchers arrived at the China attribution in part because some of the code the attackers use is similar to code attributed to other Chinese groups. Additionally, documents used in the phishing attacks were created in WPS Office or Kingsoft Office, a Chinese software similar to Microsoft Office. The Attacks The first campaign hit a government entity in Myanmar in May 2012. Mofang hacked a Ministry of Commerce server. That same month, they also targeted two German automotive companies, one engaged in developing technology for armored tanks and trucks for the military, the other involved in rocket-launching installations. In August and September 2013 they struck targets in the US. In one case, they targeted US military and government workers by emailing them a registration form for Essentials of 21st Century Electronic Warfare, a training course for US government employees held in Virginia. They also targeted a US tech company doing solar cell research as well as exhibitors at the 2013 MSME DEFExpo in India—an annual defense, aerospace and homeland security expo for companies selling to governments. In 2014 they struck an unknown South Korean organization, and in April that year they targeted a Myanmar government agency using a document purporting to be about human rights and sanctions in Myanmar. “The variety [of their targets] is big, but they always go after technology and research and development companies,” Klijnsma says. But the most telling attack came last year when they targeted a Myanmar government entity and a Singapore-based company called CPG Corporation, both of whom were involved in making decisions about foreign investments in the Myanmar special economic zone known as Kyaukphyu, which entices foreign investors with tax breaks and extended land leases. The Kyaukphyu zone was of particular interest to the China National Petroleum Corporation which began investing there in 2009. The company signed a memorandum of understanding to build a seaport and develop, operate and manage an oil and gas pipeline connecting Myanmar to China to save the Chinese company from having to sail through the Strait of Malacca to deliver gas. The Chinese government may have feared that without a binding legal agreement, Myanmar would renege on the deal. In March 2014 Myanmar chose a consortium led by the CPG Corporation in Singapore to help make decisions about development in the zone. In 2015, the consortium intended to reveal the companies that had won infrastructure investment rights but by July no results had been disclosed. That’s when the Mofang group hacked the CPG corporation, Klijnsma says. Fox-IT does not know what specific information was taken, but the timing is illustrative. “The timeline is very specific,” he says. “It lines up ridiculously well [with the decision-making period].” In 2016, China won the tender to build the oil and gas pipeline and seaport in Myanmar’s economic zone. And with that, the Mofang group’s motives seem clear.

### \*\*\*AT: Military Superiority\*\*\*

### 2AC – US Military Superiority Inevitable / No Impact

#### China won’t challenge US leadership – lacks hegemonic ambition and technological capability – interdependence ensures co-operation – [their strive for superiority ensures collapse]

Chen 15 – (Dingding Chen is an assistant professor of Government and Public Administration at the University of Macau, Non-Resident Fellow at the Global Public Policy Institute (GPPi) Berlin, Germany. He is also the Founding Director of Intellisia Institute, a newly established independent think tank focusing on international affairs in China. His research interests include: Chinese foreign policy, Asian security, Chinese politics, and human rights; 6/14/15, “Relax, China Won't Challenge US Hegemony,” *The Diplomat*, <http://thediplomat.com/2015/01/relax-china-wont-challenge-us-hegemony>, Accessed 6/27/16, HWilson)

Needless to say, the Sino-U.S. relationship is one of the most important yet complicated bilateral relationships in the world today. This explains why Chinese Vice Premier Wang Yang’s recent comments on Sino-U.S. relations have stirred up a debate online (here and here). Wang Yang stated that China “[has] neither the ability nor the intent to challenge the United States.” Partly because it is rare for a senior Chinese leader to make such soft remarks with regard to Sino-U.S. relations and partly because Wang’s remarks are seemingly inconsistent with China’s recent assertive foreign policies, there has been a fierce debate about the true meaning of Wang’s remarks in the United States. Most American analysts, however, are skeptical toward Wang’s conciliatory remarks and continue to believe that China’s ultimate aim is to establish a China-centric order in Asia at the expense of the U.S. influence in Asia. In other words, China seeks to replace the U.S. as the new global hegemon.

The reactions from the U.S. side, again, reveal the deep mistrust with regard to China’s long term goals. But such skepticism is misguided and even dangerous to Asia’s peace and stability if left uncorrected. Why? Because Wang Yang was sincere when he said that China does not have the capabilities and desires to challenge the United States. The evidence of his sincerity is apparent.

First let us look at China’s capabilities, which need to be especially formidable if China wants to challenge the United States. Although China’s comprehensive capabilities have been growing rapidly for the past three decades, almost all analysts inside and outside of China agree that there is still a huge gap between China and the U.S. in terms of comprehensive capabilities, particularly when the U.S. is far ahead of China in military and technological realms. China’s economy might have already passed the U.S. economy as the largest one in 2014, but the quality of China’s economy still remains a major weakness for Beijing. Thus, it would be a serious mistake for China to challenge the U.S. directly given the wide gap of capabilities between the two. Even if one day China’s comprehensive capabilities catch up with the United States, it would still be a huge mistake for China to challenge the U.S. because by then the two economies would be much more closely interconnected, creating a situation of mutual dependence benefiting both countries.

Besides limited capabilities, China also has limited ambitions which have not been properly understood by many U.S. analysts. It is true that China’s grand strategy is to realize the “China dream” — a dream that will bring wealth, glory, and power to China again — but this, by no means, suggests that China wants to become a hegemon in Asia, or to create a Sino-centric tributary system around which all smaller states must obey China’s orders. Perhaps these perceptions exist in the United States because many U.S. analysts have unconsciously let ultra-realist thinking slip into their minds, thereby believing that states are constantly engaged in the ruthless pursuit of power and influence. But the structure of international politics has fundamentally changed since the end of the Cold War, thus rendering any serious possibility of world hegemony ineffective or even impossible. In essence, the costs of hegemony outweigh the benefits of hegemony in this new era of international politics, thanks to rising nationalism, nuclear weapons, and increasing economic interdependence between major powers. The Chinese leaders understand this new and changed structure of international politics and based on their assessments, they have decided not to seek hegemony, which is a losing business in this new era.

Unfortunately, the U.S. is still obsessed with the concept (or illusion) of hegemony, as Simon Reich and Richard Ned Lebow have pointed out recently. The hegemony mentality is precisely the reason why the United States has declined (slowly) in the post-Cold War era. Wrongly believing that a stable global order needs U.S. hegemony, American leaders have adopted a grand strategy of liberal interventionism, which has only caused self-inflicted wounds for the U.S. economy and its global status. The tragedy, however, is that within U.S. elite circles, this misperception about U.S. hegemony (here and here) sticks and is unlikely to go away for a long time barring a major failure or crisis.

At the end of the day, our world can survive and prosper without a hegemon, regardless of whether the hegemon is American or Chinese. The sooner American leaders understand this point and believe Chinese leaders’ words, the higher the chances of peace and stability worldwide.

### ---XT: US Military Superiority Inevitable / No Impact

#### China isn’t a challenger to military leadership – their disad is Trump logic and ignores a litany of other factors that cement US military leadership

Bandow 16 – (Doug Bandow is a Senior Fellow at the Cato Institute and a former Special Assistant to President Ronald Reagan. He is a Foreign Policy Fellow and Scholar with Defense Priorities; 5/25/16, “Is China Really That Dangerous?,” *National Interest*, <http://nationalinterest.org/blog/the-skeptics/china-really-dangerous-16347?page=show>, Accessed 6/29/16, HWilson)

The United States dominates the globe militarily. Washington possesses the most powerful armed forces, accounts for roughly 40 percent of the globe’s military outlays, and is allied with every major industrialized state save China and Russia.

Yet the bipartisan hawks who dominate U.S. foreign policy see threats at every turn. For some, the People’s Republic of China is replacing the Soviet Union as America’s chief adversary. They view another military buildup as the only answer.

The PRC’s rise is reshaping the globe. Today, the PRC ranks second only to the United States economically. Increased financial resources have enabled Beijing to take on a much greater international role.

Of greatest concern in Washington is China’s military buildup. Indeed, a novel reportedly making the rounds at the Pentagon is Ghost Fleet, which posits a Chinese attack on Hawaii.

The Department of Defense publishes an annual review of China’s military. The latest report warns that the PRC “continued to improve key capabilities,” including ballistic and cruise missiles, aircraft and air defense, information capabilities, submarines, and amphibious and airborne assault units. The Chinese military “is also focusing on counterspace, offensive cyber operations, and electronic warfare.” Further, Beijing “continued to modernize and to restructure its ground forces to create a fully modern army.”

This program may sound menacing, but Beijing’s ambitions are bounded. DOD observes that China’s leaders “portray a strong military as critical to advancing Chinese interests, preventing other countries from taking steps that would damage those interests, and ensuring that China can defend itself and its sovereignty claims.” Which is precisely what U.S. policymakers do.

In the short term, Beijing’s principal objective is to advance its territorial claims in the Asia-Pacific without provoking conflict. In the longer term the objective, says DOD, is “to deter or defeat adversary power projection and counter third-party—including U.S.—intervention during a crisis or conflict.” That is, deterrence.

Most important is planning for contingencies in the Taiwan Strait, East and South China Sea, and Korean peninsula. They all concern Beijing far more than America, and involve other, potentially well-armed states, including Japan, South Korea and the Southeast Asian nations, which are able to advance their own interests.

China also is developing a capability for such missions as “sea lane security, counterpiracy, peacekeeping, and humanitarian assistance/disaster relief.” These tasks actually mirror U.S. interests. Washington officials might feel uncomfortable sharing leadership with the PRC, but that cannot justify a military response.

Most important, even the Pentagon does not believe Beijing is planning an aggressive war. America enjoys a vast military lead, possessing a significantly larger nuclear force, ten carrier groups compared to China’s single carrier and much more. With Washington spending roughly $600 billion annually on the military, compared to an estimated $180 billion by Beijing, China is not overtaking America.

Moreover, the PRC’s economic predominance is not guaranteed. China’s challenges are huge: white elephant investments, a shrinking labor force, inefficient state enterprises, ubiquitous bank bad debts, pervasive corruption and regional disparities. Because of Beijing’s one-child policy, the country may grow old before it grows rich. China’s military modernization program also faces serious challenges, including a slowing economy and pervasive corruption that afflicts the People’s Liberation Army.

Even a more powerful PRC would not easily threaten the United States. Projecting force across oceans and continents is extraordinarily expensive. Deterring use of such force is relatively cheap. America is uniquely secure, enjoying relative geographic isolation—in contrast to China, which is surrounded by nations with which it has been at war over the last century: Russia, Japan, Korea, India and Vietnam.

#### A litany of structural factors means China’s military will always remain weak and non-aggressive

Dibb 15 – (Paul Dibb is Emeritus Professor of Strategic Studies at The Australian National University, 10/15/15, “Not So Scary: This Is Why China's Military Is a Paper Tiger,” *The National Interest*, <http://nationalinterest.org/blog/the-buzz/not-so-scary-why-chinas-military-paper-tiger-14085?page=show>, originally appeared in ASPI’s The Strategist at <http://www.aspistrategist.org.au/why-the-pla-is-a-paper-tiger/>, Accessed 6/30/15, HWilson)

It’s becoming commonplace to drum up the military threat from China and belittle America’s military capabilities. Much of this commentary reminds me of statements in the mid-1980s that the former Soviet Union was poised to outstrip the U.S. in military power. This isn’t to argue that China is in the final stages of disintegration like the USSR, but it is to assert that the People’s Liberation Army (PLA) demonstrates all the brittleness and paper-thin professionalism of a military that has never fought a modern war and whose much-vaunted military equipment has never been tested in combat.

With a slowing economy, and with structural economic and social tensions becoming worse rather than better, China is a large but fragile power ruled by a vulnerable party that can’t afford any economic or foreign policy disasters, let alone war with the U.S. Its economy is fundamentally interdependent with that of free international trade and global supply chains. War for China would be an economic and social disaster.

Moreover, Beijing has very few powerful or influential friends in the region and suffers from strategic isolation, which is growing worse the more it throws its weight around.

Beijing has no experience whatsoever of modern war. Its last experience of armed conflict was in 1979 when it abysmally failed to teach Vietnam a so-called ‘lesson’. Border scuffles with India and the USSR in the 1960s and sending peasant armies into the Korean War in the 1950s scarcely rate as modern combat.

The PLA’s power depends crucially on keeping the Communist Party in power, which is what its oath of allegiance declares, and not the defense of China as a country. PLA officers still waste inordinate amounts of time learning irrelevant communist dogma, rather than giving priority to military training. Then there’s the issue of corruption at the highest levels of the PLA and the buying of favors and promotions.

It’s true that in the last several decades the PLA has made some impressive strides technologically. But despite President Xi Jinping proclaiming that China must become a powerful maritime power, geography is against it. When was the last time a large land power really made it as a naval power? Certainly not the USSR, France or Germany.

Commentators in Australia repeat a lot of breathless assertions about China’s anti-access and area denial capabilities. And there can be no doubt that operating in the approaches to China is becoming more dangerous, particularly given the sort of military mass that China can accumulate close to home. But do we actually think that the Americans are sitting on their hands doing nothing technologically in areas such as hypersonic vehicles, railguns, stealth, drones and cyber-attack?

In key areas of military technology China is still a good 20 years behind the U.S. Its anti submarine warfare capability is marginal and many of its submarines are noisy. China lacks the necessary quieting and propulsion technologies to build anything remotely comparable to an U.S. or Russian nuclear submarine. Even the newest Chinese Jin-class ballistic missile nuclear submarines are louder than the 1970s era Soviet Delta III SSBN. And the forthcoming type 95 nuclear submarine will be louder than the late-1980s Soviet titanium-hulled Akula, according to U.S. sources.

China’s air defence capabilities have gaping deficiencies against any technologically advanced enemy. Moreover, China still relies heavily on Russia for military reverse engineering and supply of high-performance military jet engines, which it has failed to master for 30 years.

Beijing has made important strides with ballistic missile technologies, but the DF-21 has never destroyed a naval target moving at battle speed. Moreover, it relies crucially on intelligence satellites and long-range over-the-horizon radar for target acquisition. Those are soft targets and vulnerable to preemptive U.S. military strikes.

It isn’t clear in any case, according to the Pentagon, whether China has the capability to collect accurate targeting information and pass it to launch platforms in time for successful strikes against distant targets at sea.

As for China’s ICBM capabilities, such as the DF-5B with multiple independently targetable re-entry vehicles (MIRVs), this is hardly a breakthrough nuclear technology. In 1974, as Head of the National Assessments Staff, I was briefed by the CIA about MIRVs on the Soviet Union’s SS-18 ICBM. That was remarkable technological advance 40 years ago.

There are some Chinese military officers and academics who are starting to brag about China’s nuclear war-fighting capabilities. While China has a reasonably secure second-strike capability, it’s one of the most vulnerable large powers to all-out nuclear war because of its population density and its distribution along the eastern seaboard. Just because China has a population 1.4 billion people doesn’t mean that it would survive a massive nuclear attack. That’s a strong argument, in my view, for the U.S. to keep a large nuclear attack force, both operational and in active reserve, of several thousand strategic warheads.

All this is to argue that we need to put China’s emerging military capabilities into some sensible comparative analysis with those of the U.S. and in historical context. We need to remember that the U.S. is the most innovative country in the world and isn’t standing still in the face of Chinese military advancements, many of which are seriously deficient.

### 2AC – China Superior Now

#### \*\*\*note when prepping file --- you can’t read both “US Military superiority inevitable” and “China Military superiority non-unique” – I just included both so that 2As can choose which to read

#### Non-unique – China’s already militarily superior despite massive U.S. spending

Francis 14 – (David Francis is a staff writer for Foreign Policy, where he oversees FP's breaking news blog, The Cable. An award-winning journalist, David has reported from all over Europe, Nigeria, Kenya, Mexico, and Afghanistan on terrorism, national security, the geopolitics of energy, global economics, and the European financial crisis; 9/16/14, “Here’s Proof We’re Losing the Arms Race to Russia and China,” *The Fiscal Times*, <http://www.thefiscaltimes.com/Articles/2014/09/16/Here-s-Proof-We-re-Losing-Arms-Race-Russia-and-China>, Accessed 6/30/16, HWilson)

The United States still has the largest defense budget in the world, some three times more than China’s and over $500 billion more than Russia’s – and it will have the largest for years to come. The nature of spending in each country, however, gives Russia and China an advantage over the United States in a brewing global arms race.

U.S. defense spending went up dramatically during the war on terror, but barring any dramatic strategy shifts, DOD spending is set to go down some $600 billion in the next decade. The chart below illustrates the trend.

Russia and China, however, are in the opposite situation as the U.S.

Both countries are in the middle of dramatic efforts to modernize their militaries. This chart shows trends in Russian military spending.

Over the next six years, Russia is also set to add some $700 billion in additional spending to the budget. So the trend you see ending in 2012 will continue well into the future.

Now, take a look at Chinese defense spending.

Like Russia, Chinese defense spending is trending up as American defense trending is trending down.

“Chinese spending in real terms after adjusting for inflation has gone up 10 to 12 percent [annually] for the past decade,” Robert Haddick, a contractor at U.S. Special Operations Command and author of Fire on the Water: China, America, and the Future of the Pacific, told The Fiscal Times. “The Chinese defense budget doubles about every 7 to 8 years in real inflation adjusted terms.”

One could make the argument that even as Russia’s and China’s spending are trending up, their budgets still pale in comparison to that of the United States. But what’s important is not how much money is being spent, but how it’s being spent.

Russia and China are investing in new state-of-the-art equipment. For instance, both countries have sleek new nuclear subs. Russia has a tank that is 14 tons lighter than the American Abrams tank but with equal capabilities. China has made great strides in drone warfare and missile technology to play enforcer in its near neighborhood. Then, there’s cyber warfare, where both China and Russia are at a decided advantage over the United States.

Meanwhile, the Pentagon is investing in failing weapons programs like the F-35 or in modernizing old weapons systems. This spending reality prompted Defense Secretary Chuck Hagel to overhaul the way the Pentagon develops technology to make it more cost effective while allowing DOD to keep up with overseas rivals.

“While the United States currently has a decisive military and technological edge over any potential adversary, our future superiority is not a given,” Hagel said in early September. “China and Russia have been trying to close the technology gap by pursuing and funding long-term, comprehensive military modernization programs.

They are also developing anti-ship, anti-air, counter-space, cyber, electronic warfare and special operations capabilities that appear designed to counter traditional U.S. military advantages.” Without changes, Haddick warned that the American strategy in Southeast Asia could become obsolete.

“It really puts in increasing jeopardy the U.S. operational concepts that the US has employed,” he said.

One thing the Chinese and Russians don’t do is waste the money they’re allotted. The DOD, on the other hand, is one of the worst abusers of taxpayer dollars.

### 2AC – China Rise Inevitable / US Decline Inev

#### The challenge to US primacy is inevitable – the US military is comparatively declining

Lemon and Johnson 16 – (Adam Lemon is a member of the Young Leaders Program at The Heritage Foundation; Justin T. Johnson is a Senior Policy Analyst for Defense Budgeting Policy at The Heritage Foundation; 6/9/16, “America's Greatest Military Nightmare Is Coming True: The Army is in Decline,” *The National Interest*, <http://nationalinterest.org/blog/the-buzz/americas-greatest-military-nightmare-coming-true-the-army-16522>, Accessed 7/1/16, HWilson)

Today, the United States and its allies face a wider and more serious array of threats than at any point since the end of the Cold War a quarter of a century ago. While the demand for troops to confront these challenges is increasing, the size and readiness of the U.S. Army is in steep decline.

Years of budget cuts have rapidly shrunk the Army to a size unseen since before World War II. The preparedness of the troops has been damaged as well. The Army has been forced to cut training and next-generation weapons programs that are vital for preparing the force for 21st century conflict.

General Daniel B Allyn, the Vice Chief of Staff of the Army has witnessed firsthand the damage done by the defense budget cuts. Allyn will discuss the state of the U.S. Army at the Heritage Foundation on Monday June 13. Before rising to the number two position in the Army, Allyn served in a number of combat commands and is uniquely positioned to discuss the serious challenges facing the U.S. Army.

In 2011 the Army had more than 566,000 active duty personnel. By the end of this summer, that number will be around 475,000 due to budget cuts. That smaller force will be called upon to do far more tasks than it did in 2011.

Among these will be training and reassuring allies, destroying ISIS, and deterring Russia, China, and Iran. This is all in addition to maintain a lasting presence in Afghanistan. The decline in numbers will continue through 2018, when the Army is expected to bottom out at 450,000 troops.

This decline is even more troubling when considering the number of Brigade Combat Teams, the building block of deployable Army forces. The Army totaled 45 Brigade Combat Teams of active duty personnel in 2013. By the end of 2018 there will be only 30. While the Brigade Combat Teams have been reorganized to increase combat power, a 20 percent decline in troops is causing a 33 percent decline in BCTs, thus the Army will have fewer units to rotate through an increasing number of operational tasks.

Since budget cuts began, the Army’s readiness to deploy and fight effectively in the event of conflict has suffered dramatically.

The Pentagon has tried to remedy this by decreasing or cutting funding to several Army weapons modernization programs in order to better fund readiness and training. Yet with all this effort, according to Pentagon officials only one third of active and reserve Army Brigade Combat Teams are sufficiently ready for combat. Of the roughly 20 active and reserve BCTs that are ready for combat, 11 are already assigned to combatant commands,leaving only 9 BCTs for unforeseen contingencies.

In addition to poor readiness in general, the Army has focused so much on dealing with insurgencies in Iraq and Afghanistan that it is ill-prepared for conflict with conventional threats like the rapidly expanding and modernizing militaries of Russia and China.

As Congress debates the 2017 defense authorization bill, it must recognize that the Army is smaller, faces greater threats in more varying regions of the world, and is ill-prepared to fight a modern war. Our military commanders have been raising the alarm, but Congress is yet to act decisively.

### ---XT: China Rise Inevitable

#### Chinese military modernization’s high now – independently non-uniques the disad

Davis 15 – (Malcolm Davis is assistant professor in International Relations and post-doctoral research fellow in China-Western Relations at Bond University, 10/22/15, “Get Ready, Asia: China's Military Is Rapidly Catching Up to America,” <http://nationalinterest.org/blog/the-buzz/get-ready-asia-chinas-military-rapidly-catching-america-14147?page=show>, Accessed 6/29/16, HWilson)

In considering Paul Dibb’s analysis on the Chinese People’s Liberation Army (PLA), I’d recommend anyone interested in the state of China’s military start by reading Roger Cliff’s China’s Military Power: Assessing Current and Future Capabilities. Cliff argues that “…by 2020, the quality of China’s military doctrine, equipment, personnel and training will likely be approaching, to varying degrees, those of the US and other Western militaries.”

Although prevailing weaknesses in organizational structure, logistics and organizational culture will limit the effectiveness of PLA weapons and platforms, “defeating China in these scenarios [Taiwan and South China Sea] could nonetheless be difficult and costly for the United States’ primarily as a result of the geographic advantages that China enjoys, as well as specific systems capabilities.”

Finally, he suggests, “the 2020s are likely to be a time of power transition in East Asia, from a region in which the United States has had the capability to defend its allies against virtually any form of aggression, to one where China has the capability to, at a minimum, contest control of the seas and airspace and where an attempt to oppose a Chinese use of force will be dangerous and costly for any country, including the United States.”

Cliff’s conclusion is also echoed in a recent RAND report, “The US China Military Scorecard,” which argues that China is catching up to the U.S., is becoming more assertive and confident, and has geography on its side. The report notes that “China [has been able] to narrow the military gap in almost every area and move ahead in some” and that the “overall capability trend lines are moving against the United States.” The report also highlights the speed of change in China’s military: it’s pushing forward in key capability areas and its modernization is occurring more rapidly than that of the U.S. China is leapfrogging, whilst the U.S. is plodding.

These two accounts suggest worrying trends and highlight that an analysis of the PLA which is based on superficial glimpses of selected areas of capability misses the bigger picture. The speed of China’s military modernization, its sustained investment in terms of double-digit spending levels, and the types of capabilities it is acquiring highlight China’s strategic objective of eroding America’s military–technological advantage so that Beijing may resolve territorial disputes and ensure the success of the China Dream.

Even though China does face real domestic challenges, so does the U.S. in the form of growing national debt and destructive political partisanship in Washington that together reduces its ability to sustain defence spending in coming years to offset Chinese capability growth. That’s occurring as security risks in Europe and the Middle East multiply to impose greater burdens on shrinking forces. The end result is reduced U.S. readiness and overall effectiveness at a critical time later this decade.

Paul’s dismissal of PLA capabilities seems to lack operational context and overlook PLA capabilities now in service. A key emerging issue is the survivability of naval surface forces in the face of PLA anti-access-area-denial (A2/AD) capabilities. Here PLA ability to wage information warfare against vital U.S. C4ISR networks through counter-space operations with ASATs, integrated network-electronic warfare (INEW), and cyber warfare need to be considered more deeply as winning the information battle against China is vital to countering their A2/AD capabilities. The RAND report notes that Chinese offensive counterspace capability, for example, is growing faster than the U.S. defensive counter-space options. There may be technological silver bullets to mitigate such developments but they must first be funded through to operational status, and then proven to work in battle.

While Paul is certainly correct to suggest that the U.S. isn’t ‘sitting on its hands’ as its ‘Third Offset’ strategy clearly demonstrates, this argument can also be reversed. China has flown hypersonic glide vehicles, is deploying counter-stealth radars, and has the world’s largest unmanned air vehicle capability.

China is catching up in anti-submarine warfare, with the deployment of fixed acoustic arrays and Jingdao class ASW corvettes, as well as new maritime patrol aircraft. In air defence, China will likely acquire the S-400 SAM which is effective against stealth aircraft, and long-range air combat capabilities epitomised by the J-20 can exploit the U.S. reliance on forward-deployed AEW&C and airborne refuelling aircraft to further reduce US ability to project airpower.

In terms of submarine quieting, nuclear submarines are always going to be noisier than conventional boats. China deploys both the Yuan and Kilo 636 conventional submarines which are very quiet and difficult to detect in acoustically challenging waters in the South China Sea. The RAND report notes that “China’s newer submarines are becoming quieter and better armed, and there is every reason to believe that their capability to find and attack U.S. surface ships has vastly improved [since 1996].” It is the ability of these boats to fire long-range supersonic anti-ship cruise missiles (ASCMs), such as the new 290nm range YJ-18, that according to Andrew Erickson allow China to “out-stick” the U.S. in long-range anti-surface warfare. This submarine-ASCM combination is quite deadly.

Paul Dibb is correct to caution against seeing the PLA as ten feet tall, but it would be equally unwise to dismiss China as inconsequential in military-technological terms. China is rapidly catching up, and what matters is where the PLA goes from here, and how Beijing uses its growing military power across Asia.

#### Chinese submarines upset the military balance and thump the internal link

Majumdar 16 – (Dave Majumdar is the defense editor of The National Interest; 6/27/16, “Why the US Navy Should Fear China's New 093B Nuclear Attack Submarine,” *The National Interest*, <http://nationalinterest.org/blog/the-buzz/why-the-us-navy-should-fear-chinas-new-093b-nuclear-attack-16741?page=show>, Accessed 7/1/16, HWilson)

Is China’s new Type 093B nuclear-powered attack submarine on par with the U.S. Navy’s Improved Los Angeles-class boats?

At least some U.S. naval analysts believe so and contend that the introduction of the new People’s Liberation Army Navy (PLAN) submarines is an indication of just how quickly Beijing is catching up to the West.

“The 93B is not to be confused with the 93. It is a transition platform between the 93 and the forthcoming 95,” said Jerry Hendrix, director of the Defense Strategies and Assessments Program at the Center for a New American Security—who is also a former U.S. Navy Captain. “It is quieter and it has a new assortment of weapons to include cruise missiles and a vertical launch capability. The 93B is analogous to our LA improved in quietness and their appearance demonstrates that China is learning quickly about how to build a modern fast attack boat.”

Other sources were not convinced that Beijing could have made such enormous technological strides so quickly—but they noted that the topic of Chinese undersea warfare capability is very classified. Open source analysis is often extremely difficult, if not impossible. “Regarding the question on the Type 093B, I really don’t know, anything is possible I suppose, but I doubt it,” said retired Rear Adm. Mike McDevitt, now an analyst at CNA’s Center for Naval Analyses. “I have no doubt that the PLAN has ambitions to at least achieve that level of capability and quietness.”

Though the Seawolf and Virginia-classes have surpassed the Improved Los Angeles-class as the premier U.S. Navy attack submarines, such older vessels will remain the mainstay of the service’s undersea fleet for many years to come. If the People’s Liberation Army Navy’s newest boats are able to match the capabilities of the U.S. Navy’s shrinking undersea fleet, Washington could be in serious trouble. Indeed, the U.S. Navy already anticipated that it could be facing-off against a Chinese submarine fleet that is nearly twice its size, but not as technically capable.

The U.S. Navy—which has roughly 52 attack submarines—is on track to have 41 attack boats by 2029. The Chinese, meanwhile would have “at least 70, and they’re building,” Vice Adm. Joseph Mulloy, the service’s deputy chief of naval operations for integration of capabilities and resources told the House Armed Services Committee’s seapower and projection forces subcommittee on February 25. “You get back into the whole quality versus quantity issue, but at the same time the Russians are also building...and they build much higher-end submarines.”

In a 2016 report to Congress, the Pentagon noted that Beijing continues to upgrade and expand its submarine fleet: “China continues to improve its SSN force, and four additional SHANG-class SSN (Type 093) will eventually join the two already in service. The SHANG SSN will replace the aging HAN class SSN (Type 091). These improved SHANG SSNs feature a vertical launch system (VLS) and may be able to fire the YJ-18 advanced anti-ship cruise missile (ASCM). Over the next decade, China may construct a new Type 095 nuclear-powered, guided missile attack submarine (SSGN), which not only would improve the PLAN’s anti-surface warfare capability but might also provide it with a more clandestine land-attack option.”

The problem, however, is if Hendrix’s assessment is correct and future Chinese submarines are only slightly less capable than the Virginia or Seawolf-class vessels, the Navy could be in trouble. The technological edge the U.S. Navy—which is already woefully short on attack boats—is counting on might not be sufficient to counter Chinese numerical superiority. However, the service is continuing to improve the performance capabilities of its submarines on a continual basis. Nonetheless, one former U.S. Navy undersea warfare officer suggested that the service would come to regret having truncated the high-performance submarine-hunting Seawolf-class at three boats and focusing instead on the more multi-role Virginia-class.

#### Relative U.S. decline is inevitable – 6 warrants

Johnson 16 – (Justin T. Johnson is a Senior Policy Analyst for Defense Budgeting Policy at The Heritage Foundation, 3/18/16, “6 Signs the U.S. Military Is Dying a Slow, Painful Death,” *The National Interest*, <http://nationalinterest.org/blog/the-buzz/6-reasons-the-us-military-dying-slow-painful-death-16252?page=show>, Accessed 7/1/16, HWilson)

The U.S. military seems to be breaking.

Senior military leaders have made dire statements before Congress, and story after story is revealing the potentially deadly challenges facing our men and women in uniform.

As Congress considers the annual defense authorization bill, here are six clear, real-world examples of why Congress needs to use the defense bill to start rebuilding the U.S. military.

1. The Marine Corps is pulling parts off of museum planes to keep their F-18s flying. Even with that drastic action, only about 30 percent of their F-18s are ready to fly. Not only that, but instead of getting 25 or 30 hours a month in the cockpit, Marine Corps pilots are getting as little as four hours per month of flying time.

2. Only one-third of Army brigades are ready for combat. The Army has now fallen to the smallest level since before World War II, while the top Army general says that the Army would face “high military risk” if it were to fight a serious war.

3. The Air Force is cannibalizing parts from some F-16’s to keep other F-16’s flying and is pulling parts off museum planes to keep their B-1 bombers flying. And half of Air Force squadrons are not prepared for serious combat.

4. The Navy keeps extending deployments of its ships, but still doesn’t have enough to meet demand. While the Navy needs about 350 ships, today it only has 273.

5. Serious crashes of Marine Corps planes and helicopters are nearly double the 10-year average.

6. The Air Force’s B-52 bombers are an average of 53 years old. Most Americans would not want to drive across the country in a 53-year-old car (see example below), let alone go to combat in a 53-year-old airplane.

These six facts show the consequences of cutting the national defense budget by 25 percent over the last five years.

At the same time, threats are growing. Russia has invaded Ukraine and threatens more. China is building illegal islands. Iran is pursuing a nuclear weapon and North Korea already has one. And we also face the real threat of terrorism and the growing threat of cyberattacks.

### \*\*\*AT Semiconductors\*\*\*

### 2AC – Non-Unique

#### Non-unique – China has a surplus of semiconductors now

Mims 13 – (Christopher Mims is the science and technology correspondent for Quartz. He is a former editor at Seed, Scientific American, Technology Review, Grist and Smithsonian, he spent a decade writing news and analysis for the aforementioned, as well as BBC, Wired, Nature and the like; 4/9/13, “China just surpassed the US in semiconductor manufacturing—and the trend is likely to accelerate,” *Quartz*, <http://qz.com/72542/china-just-surpassed-the-us-in-semiconductor-manufacturing-and-the-trend-is-likely-to-accelerate/>, Accessed 6/29/16, HWilson)

For the first time since the depths of the Great Recession, the the total value of materials consumed by all the world’s makers of microchips was down—2%, to $47.11 billion. But that’s just one of the stories told by data from the annual tabulation of the total value of materials consumed by all the world’s makers of microchips, compiled by industry association SEMI.

Assembling data from SEMI’s last four annual reports—which together cover the past 5 years, a number of trends are apparent.

China is now a bigger consumer of the raw materials used for making microchips than North America is.

This is a huge change from 2008, when China consumed only $3.57 billion of silicon ingots and the other materials used for semiconductor manufacture, compared to $4.99 billion consumed by North America. This means that the number and productivity of plants for making microchips—which are high-investment, high-tech, finished product type manufacturing operations requiring a high level of expertise—are expanding in China even as they decline in North America. Compared to 2008, consumption of semiconductor materials in North America is down $250 million to $4.74 billion, while in China consumption has shot up 42% to $5.07 billion.

The decline of the PC is probably to blame for the overall drop in consumption of microchip materials in 2012.

In 2012, manufacturers shipped record numbers of mobile devices. Demand for set-top boxes and embedded systems (e.g. industrial control systems and the computers that go into cars) remained soft on account of a troubled global economy, but to see a drop in semiconductors shipped in the absence of an outright recession suggests that what’s really going on here is the decline of the PC—and the expensive, materials-hungry processors and memory it incorporates.

Production of microchips in Japan is declining rapidly.

What a difference five years makes. Japan, in 2008 the world’s most rapacious consumer of semiconductor materials, has seen production crash, especially in the 2011-2012 period—down 8% to $8.35 billion. Compare that with nearly $10 billion in 2008.

The harder it is to make microchips, the more consolidation there is in the hands of fewer manufacturers.

From 2011 to 2012, consumption of microchip precursor materials was flat or down in every region except for China and Taiwan. Taiwan has come to dominate this industry, with contract manufacturers like Taiwan Semiconductor Manufacturing Company churning out chips for countless chip design companies that do not own their own manufacturing facilities—including mobile and telecommunications giants like Qualcomm and now, Apple.

What’s going on here is that, as we approach the end of Moore’s Law—which says, essentially, that we can expect microchips to improve at a rapid clip on a predictable timetable—we are reaching the physical limits of current manufacturing. That means factories are more expensive than ever, with price tags into the billions for a single facility. If a manufacturer wants the latest and fastest chip technology, there are only a few companies that can play at that level, and you can count them on one hand: TSMC in Taiwan, Intel and Global Foundries in North America, and Samsung in South Korea.

Consumption of microchips in China is exploding—and more and more of them are being sourced locally.

In 2012, China consumed 33% of the world’s integrated circuits (i.e. microchips) while the US consumed only 13.5%. Much of that, of course, is incorporated into products that will ultimately be exported—like iPhones. China’s share of world microchip consumption came to $137.5 billion in 2012, according to SEMI China. Meanwhile, the total value of microchips produced in China was only $28.5 billion. Closing that gap are companies like Semiconductor Manufacturing International (SMIC), Shanghai Huali Microelectronics (HLMC), Shanghai HuaHong NEC Electronics Company (HHNEC), Grace Semiconductor Manufacturing and Advanced Semiconductor Manufacturing (ASMC).

In the long run, the general emphasis on electronics manufacturing in China, along with this gap between production and demand, indicates that China is, as usual, the sleeping giant in this field. While mainland China’s production of microchips lags behind most other regions, in 2012 it saw the biggest percentage growth in consumption of microchip materials and matched the absolute value of growth in Taiwan, the only other region that saw growth last year.

Here’s the thing about microchips: China’s government views them, rightly, as an important strategic asset. It’s a stretch to compare them to, say, oil, but they are clearly very important in our increasingly connected world. It’s hard to imagine a future in which they are any less important an economic enabler than they are now. So the overall trend in where they are manufactured has implications for everything from national defense to overall competitiveness in high tech.

### 2AC – Alt Causes

#### Alt causes to semiconductor capabilities outweigh

Chu 16 – (Dr Ming-chin Monique Chu is Lecturer in Chinese Politics, Employability Officer within Social Sciences: Politics & International Relations at the University of Southampton, gained MPhil and PhD degrees in international relations from the University of Cambridge; 3/23/16, “China’s Ambitions in the Semiconductor Sphere and Taiwan’s Dilemma,” <https://sotonpolitics.org/2016/05/23/chinas-ambitions-in-the-semiconductor-sphere-and-taiwans-dilemma/>, Accessed 6/29/16, HWilson)\*\*\*note – the URL cited above is from a translation of this article originally published in Chinese at BBC News: <http://www.bbc.com/zhongwen/trad/china/2016/05/160506_china_semicounductor_business#orb-footer>

Admittedly, the Chinese ambitions to enhance its domestic semiconductor capability are not without challenges, despite the tremendous state-led endeavours to establish national champions. These include, for instance, the abilities of local firms to innovate, the reluctance by foreign firms to transfer their core technologies to China, and the obstacles faced by local firms to acquire foreign giants due to national security concerns on the part of foreign governments.